MANUAL

Versão: 26/09/14

AKER Report Center

AKER

www.aker.com.br

Indice

Indice **2**

Indice de Figuras **5**

1 Aker Report Center **11**

1.1 Como está disposto este manual. 11

1.2 Apresentação do Produto 11

2 Instalação **14**

2.1 Instalação via interface texto 14

2.2 Adicionando espaço em disco - LVM 26

2.3 Assistente de Configuração do Aker Report Center 30

2.4 Licenciamento 33

3 Dashboard **39**

3.1 Aba Dashboard 39

3.2 Aba Relatórios 42

3.2.1 Visualizando um relatório 43

3.2.2 Exportando um relatório 46

3.3 Aba Relatórios Recebidos 47

3.4 Aba Aker Monitoring 50

3.5 Aba Pesquisa 51

4 Relatórios **54**

4.1 Agendamento 54

4.1.1 Relatórios gerados 54

4.1.2 Agendar 55

4.1.3 Agendando um novo relatório 55

4.2 Relatórios gerados 57

4.3 Criar Relatório 58

4.3.1 Criando um novo tipo de relatório 58

4.3.2 Aba Relatório 59

4.3.3 Aba Fonte de dados 59
4.3.4 Aba Colunas 60
4.3.5 Aba Parâmetros 61
4.4 Grupos de relatórios 62
4.4.1 Criando um novo grupo de Relatório 62
4.5 Logs do sistema 63
5 Configurações 65
5.1 Entidades 65
5.2 Ativos 67
5.2.1 Cadastro de Ativos 67
5.2.2 Cadastrando um novo Ativo 67
5.2.3 Aba Cadastro de ativo 68
5.2.4 Aba Eventos Processados 72
5.2.5 Aba Eventos Não Processados 72
5.2.6 Colunas 73
5.2.7 Tipos de ativo 74
5.2.8 Adicionando um novo tipo de ativo: 74
5.3 Relatórios 78
5.3.1 Customização 78
5.3.2 Preferências de exportação de dados 78
5.4 Segurança 79
5.4.1 Perfis 79
5.4.2 Usuários 79
5.4.1 Configurações FTP TLS 79
5.4.2 Syslog TLS 80
5.4.3 Usuários FTP 81
5.4.4 Tipo de autenticação 82
5.5 Rede 83
5.5.1 Interfaces de rede 83

5.5.2 Servidores NTP 85
5.6 *Backup* 85
5.6.1 Realizar backup 85
5.6.2 Restaurar backup 86
5.7 *Licenciamento* 87
5.7.1 Gerar Chave 88
5.7.2 Aplicar Licença 88
5.8 Outras Configurações 90
5.8.1 Exportação de dados 90
5.8.2 Rotate 93
5.8.3 Atualizações 94
5.8.4 E-mail 95
5.8.5 Serviços 97
5.9 Ajuda 98
5.10 Opções de gerenciamento da conta do usuário 98

Indice de Figuras

Figura 1 - boot menu 14
Figura 2 - seleção de idioma 15
Figura 3 - configuração do teclado 16
Figura 4 - Carregando componentes adicionais 16
Figura 5 - Configurar a rede “nome da maquina” 17
Figura 6 - Configurar a rede "nome do domínio" 17
Figura 7 - Configurar usuários e senha 18
Figura 8 - confirmação de senha 18
Figura 9 - Nome completo para o novo usuário 18
Figura 10 - Nome de usuário para sua conta 19
Figura 11 - senha para novo usuário 19
Figura 12 - confirmação de senha 19
Figura 13 - configuração do relógio 20
Figura 14 - Particionar discos 20
Figura 15 - seleção de disco a ser particionado 21
Figura 16 - Esquema de particionamento 21
Figura 17 - Finalizar o particionamento e escrever as mudanças no disco 22
Figura 18 - Confirmação e mudanças 22
Figura 19 - instalando o sistema 22
Figura 20 - Método de codificação do console 23
Figura 21 - seleção de conjunto de caracteres 24
Figura 22 - configurar o gerenciador de pacotes 24
Figura 23 - configurando o apt 24
Figura 24 - instalar o carregador de inicialização GRUB 25
Figura 25 - Instalando o carregador de inicialização GRUB 25

Figura 26 - Finalizar a instalação 25
Figura 27 - Visualizando IP para acesso no browser 26
Figura 28 - Informações Gerais 30
Figura 29 - Banco de dados 31
Figura 30 - Informações do Administrador 32
Figura 31 - Finalizando a Instalação 32
Figura 32 - Finalizando os processos 32
Figura 33 - Mensagem de reinicialização do sistema 33
Figura 34 - Mensagem ao errar a senha mais de 3 vezes 33
Figura 35 - Tela de login 34
Figura 36 - Gerar chave 34
Figura 37 - Localizando lincença 35
Figura 38 - Opções de carregamento da licença 35
Figura 39 - Informação da licença 36
Figura 40 - Menus 37
Figura 41 - Abas do Dashboard 39
Figura 42 - Aba Dashboard 40
Figura 43 - Widgets atualizados em tempo real 40
Figura 44 – Widget “Total de eventos” 41
Figura 45 - Opções de período 41
Figura 46 - Widget "espaço utilizado em disco" 41
Figura 47 - Opções de Widget 42
Figura 48 - Aba Relatórios 43
Figura 49 - Visualização de Relatórios 44
Figura 50 - Botão pesquisar 44
Figura 51 - Modelo de relatório (Volume de download por URL) 45
Figura 52 - Modelo de relatório (Detalhes de acessos as URLs) 45

Figura 53 - Modelo de relatório (TOP 10 usuários com mais tempo de tráfego) 46
Figura 54 - Visualização de relatório ..... **Erro! Indicador não definido.**
Figura 55 - Botão Exportar 47
Figura 56 - Opções de formato de Relatório 47
Figura 57 - Exportação de relatório (PDF) 47
Figura 58 - Aba Pesquisa 52
Figura 59 - Resultado da pesquisa 52
Figura 60 - Opções do menu Relatórios 54
Figura 61 - Relatórios gerados 54
Figura 62 - Agendamento de relatório 55
Figura 63 - Agendamento de relatórios 56
Figura 64 - Opções de parâmetros de pesquisa 57
Figura 65 – Operador 57
Figura 66 - Relatórios gerados 58
Figura 67 - Relatórios 58
Figura 68 - Aba Relatório 59
Figura 69 - Aba Fonte de dados 60
Figura 70 - Aba Colunas 60
Figura 71 - Aba Parâmetros de filtro 61
Figura 72 - Opções de parâmetros de pesquisa 61
Figura 73 - Operador 62
Figura 74 - Grupos de relatórios 62
Figura 75 - Criando novo grupo de relatório 62
Figura 76 - Logs do sistema 63
Figura 77 - Opções do menu Configurações 65
Figura 78 - opções do submenu Ativos 67
Figura 79 - Cadastro de ativos 67

Figura 80 - Aba Cadastro de ativo 68
Figura 81 - Configuração de envio via FTP 69
Figura 82 - Envio Syslog 70
Figura 83 - Parâmetros de configuração 71
Figura 84 - Aba log 71
Figura 85 - Aba Eventos processados 72
Figura 86 - Aba Eventos não processados 73
Figura 87 - Colunas 73
Figura 88 - Opções de colunas 74
Figura 89 - Opções de tipos de dados 74
Figura 90 - Tipos de ativos 74
Figura 91 - Adicionando um novo tipo de ativo 75
Figura 92 - Adicionando um novo tipo de log 76
Figura 93 - Seleção de campos 77
Figura 94 - Campo de expressões regulares 77
Figura 95 - Personalização do sistema 78
Figura 96 - Preferências de exportação de dados 78
Figura 97 - Janela Perfis 79
Figura 98 - Usuários 79
Figura 99 - Configuração de segurança FTP 80
Figura 100 - Syslog TLS 81
Figura 101 - Usuários FTP 81
Figura 102 - Cadastro de usuário FTP 82
Figura 103 - Autenticação 83
Figura 104 - Janela de configuração de rede 84
Figura 105 - Servidores NTP 85
Figura 106 - Opções de backup 85

Figura 107 - Janela Realizar Backup 86
Figura 108 - Criação de backup 86
Figura 109 - localizando arquivo de backup 87
Figura 110 - Janela Restaurar Backup 87
Figura 111 - Gerar chave 88
Figura 112 - Aplicar licença 88
Figura 113 - Localizando licença 89
Figura 114 - Opções para carregar licença 89
Figura 115 - Informações da licença após aplicada 90
Figura 116 - Outras configurações 90
Figura 117 - Esquema de exportação de dados 91
Figura 118 - Janela Agendar exportação de dados 92
Figura 119 - Janela de cadastro de ativo 93
Figura 120 - Rotate 94
Figura 121 - Atualizações 95
Figura 122 - Opções para baixar atualizações 95
Figura 123 - Configurações de e-mail 96
Figura 124 - Janela de configuração de serviços 97
Figura 125 - Menu Ajuda 98
Figura 126 - Opções do usuário 98
Figura 127 - Minha conta 99
Figura 128 - Alterar Senha 99

Aker Report Center

1 Aker Report Center

Seja bem-vindo ao manual do usuário do Aker Report Center

Nos próximos capítulos você aprenderá como configurar esta poderosa ferramenta de gerenciamento de logs e criação de relatórios. Esta introdução tem como objetivo descrever a organização deste manual e tentar tornar sua leitura o mais simples e agradável possível.

1.1 Como está disposto este manual.

Este manual está organizado em vários capítulos. Cada capítulo mostrará um aspecto da configuração do produto e todas as informações relevantes ao aspecto tratado.

Todos os capítulos começam com uma introdução teórica sobre o tema a ser tratado seguido dos aspectos específicos de configuração do **Aker Report Center**. Juntamente com esta introdução teórica, alguns módulos possuem exemplos práticos do uso do serviço a ser configurado, em situações hipotéticas, porém bastante próximas da realidade. Buscamos com isso tornar o entendimento das diversas variáveis de configuração o mais simples possível.

Recomendamos que este manual seja lido pelo menos uma vez por inteiro, na ordem apresentada. Posteriormente, se for necessário, pode-se usá-lo como fonte de referência (para facilitar seu uso como referência, os capítulos estão divididos em tópicos, com acesso imediato pelo índice principal. Desta forma, pode-se achar facilmente a informação desejada).

Em vários locais deste manual, aparecerá o símbolo seguido de uma frase escrita em letras vermelhas. Isto significa que a frase em questão é uma observação muito importante e deve ser totalmente entendida antes de prosseguir com a leitura do capítulo.

1.2 Apresentação do Produto

Se a sua rede fosse vítima de um acesso não autorizado, como você iria detectar? Como você irá reagir a tal ataque antes que fosse tarde para a proteção e integridade das informações de sua empresa? Você seria capaz de rastrear a origem do ataque? E se este ataque fosse de um usuário com acesso privilegiado tentando causar algum dano à sua rede, como você iria descobrir?

Apesar da grande quantidade de dados armazenados nas maquinas das redes terem informações que são de extrema importância para a proteção e o gerenciamento de

ameaças de sua rede, a maioria das empresas não possuem os recursos necessários para usar estes dados para analisar todas estas informações efetivamente e em tempo real para proporcionar maior segurança aos dados de sua empresa.

Visando oferecer maior proteção à segurança da informação de seus clientes a **Aker Security Solutions** desenvolveu o **Aker Report Center**, uma poderosa ferramenta que oferece a você e sua rede gerenciamento de logs, análise preditiva capaz de descobrir padrões suspeitos nos dados que os olhos humanos não conseguem ver, geração de relatórios de diversos modelos de acordo com a necessidade de sua empresa nos formatos **HTML**, **TXT** e **PDF**, visualização de relatórios e gráficos personalizados, filtragem de logs customizada, agendamento de geração de relatórios, acesso seguro e flexibilidade, recebendo dados não apenas dos produtos da Aker Security Solutions (Aker Firewall 6.5 e 6.7), mas também das principais soluções de segurança da informação disponíveis no mercado.

Características

Suporta mais de 370 tipos de ativos;

- Relatórios em HTML, PDF e TXT;
- Integração com ativos de terceiros;
- Dashboard personalizável e responsivo.

Vantagens

- Alta performance;
- Ambiente escalável e flexível;
- Interface Web de fácil configuração e em português;
- Gerenciamento de logs via dispositivo móvel;
- Simplificação da gestão da infraestrutura de TI.

Instalação

2 Instalação

Neste capitulo vamos abordar a instalação, e o licenciamento do Aker Report Center.

2.1 *Instalação via interface texto*

A interface texto do Aker Report Center é instalada em uma plataforma Debian 64-bits.

Figura 1 - boot menu

Na tela inicial do instalador do Aker Report Center selecione o modo que deseja fazer a instalação, e pressione a tecla "***Enter***". A instalação exibida a seguir é baseada na instalação via texto.

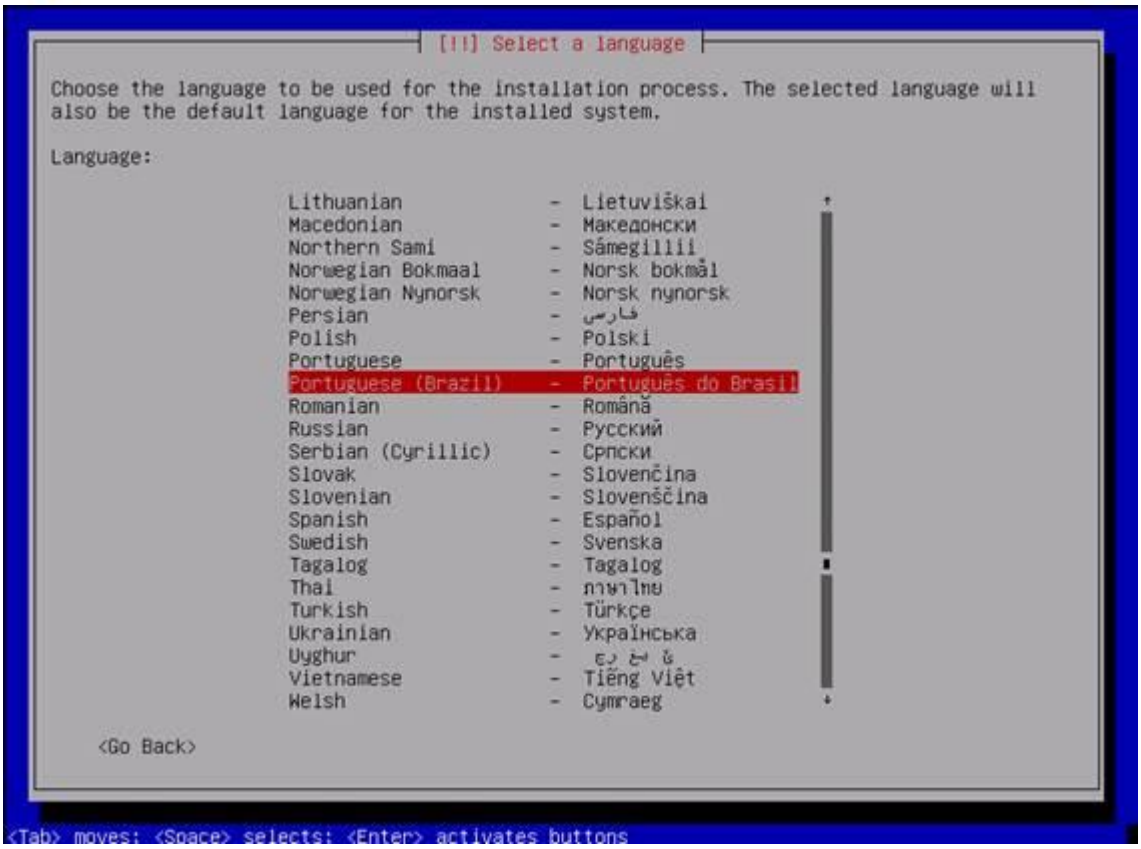

[!!] Select a language
Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.
Language:
Lithuanian - Lietuviškai
Macedonian - Македонски
Northern Sami - Sámegillii
Norwegian Bokmaal - Norsk bokmål
Norwegian Nynorsk - Norsk nynorsk
Persian - فارسی
Polish - Polski
Portuguese - Português
Portuguese (Brazil) - Português do Brasil
Romanian - Română
Russian - Русский
Serbian (Cyrillic) - Српски
Slovak - Slovenčina
Slovenian - Slovenščina
Spanish - Español
Swedish - Svenska
Tagalog - Tagalog
Thai - ภาษาไทย
Turkish - Türkçe
Ukrainian - Українська
Uyghur - ئۇيغۇرچە
Vietnamese - Tiếng Việt
Welsh - Cymraeg
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons

Figura 2 - seleção de idioma

Nesta tela o usuário deve selecionar o idioma que a instalação será feita. Selecione o idioma desejado e pressione a tecla "***Enter***".

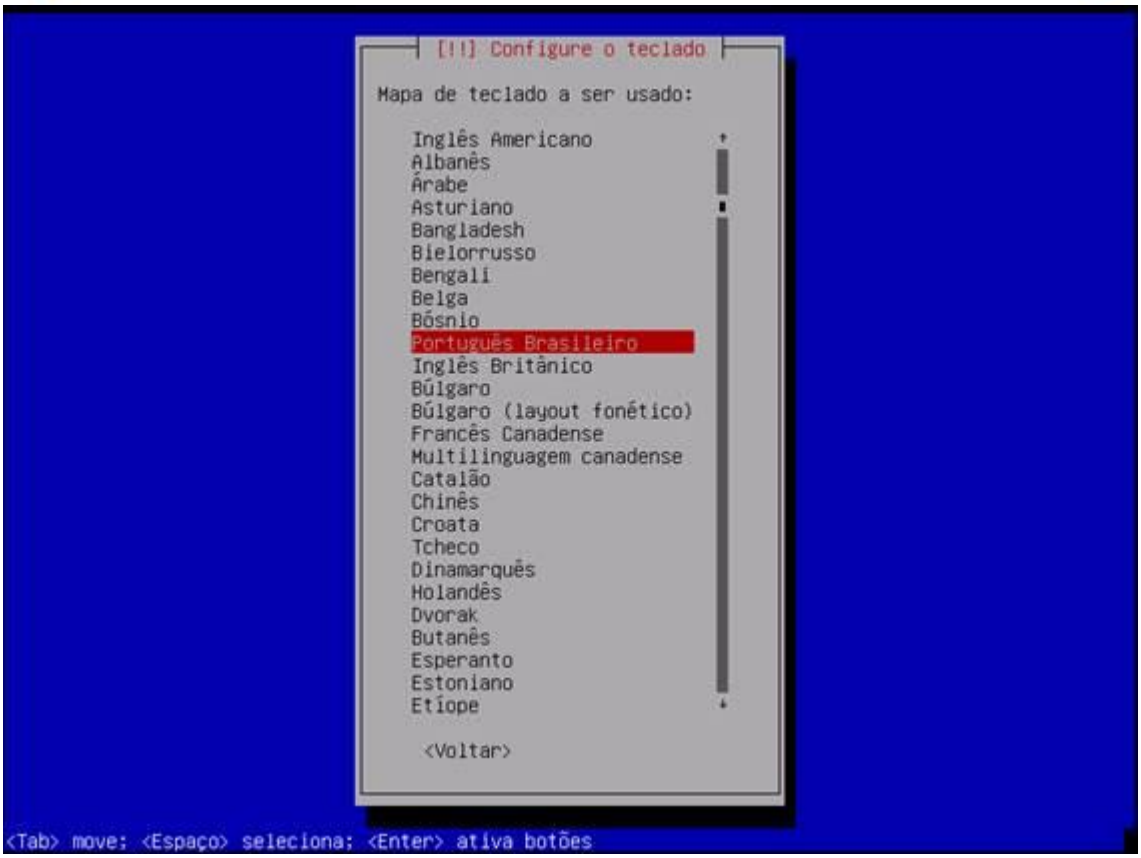


Figura 3 - configuração do teclado

Nesta tela o usuário deve selecionar o idioma de configuração do teclado. Selecione o idioma desejado e pressione a tecla "***Enter***".

Figura 4 - Carregando componentes adicionais

Aguarde o carregamento dos componentes adicionais e prossiga para a configuração da rede.

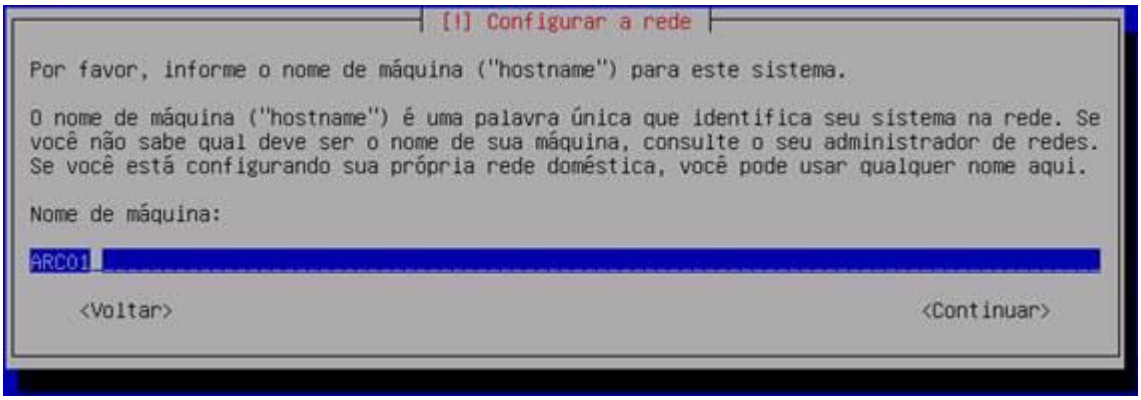

[!] Configurar a rede
Por favor, informe o nome de máquina ("hostname") para este sistema.
O nome de máquina ("hostname") é uma palavra única que identifica seu sistema na rede. Se você não sabe qual deve ser o nome de sua máquina, consulte o seu administrador de redes. Se você está configurando sua própria rede doméstica, você pode usar qualquer nome aqui.
Nome de máquina:
ARCO1
<Voltar>
<Continuar>

Figura 5 - Configurar a rede “nome da maquina”

Nesta tela o usuário deve selecionar o nome da máquina para seu sistema. Selecione o nome desejado e pressione a tecla “***Enter***”.

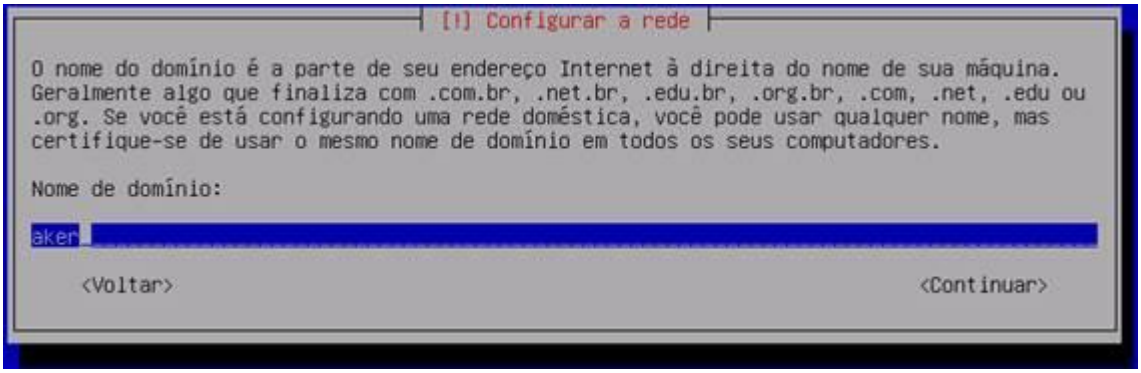

[!] Configurar a rede
O nome do domínio é a parte de seu endereço Internet à direita do nome de sua máquina. Geralmente algo que finaliza com .com.br, .net.br, .edu.br, .org.br, .com, .net, .edu ou .org. Se você está configurando uma rede doméstica, você pode usar qualquer nome, mas certifique-se de usar o mesmo nome de domínio em todos os seus computadores.
Nome de domínio:
aker
<Voltar>
<Continuar>

Figura 6 - Configurar a rede "nome do domínio"

Nesta janela o usuário pode inserir o nome do domínio de sua rede, caso não possua um domínio simplesmente deixe este campo em branco e pressione a tecla “***Enter***” para continuar.

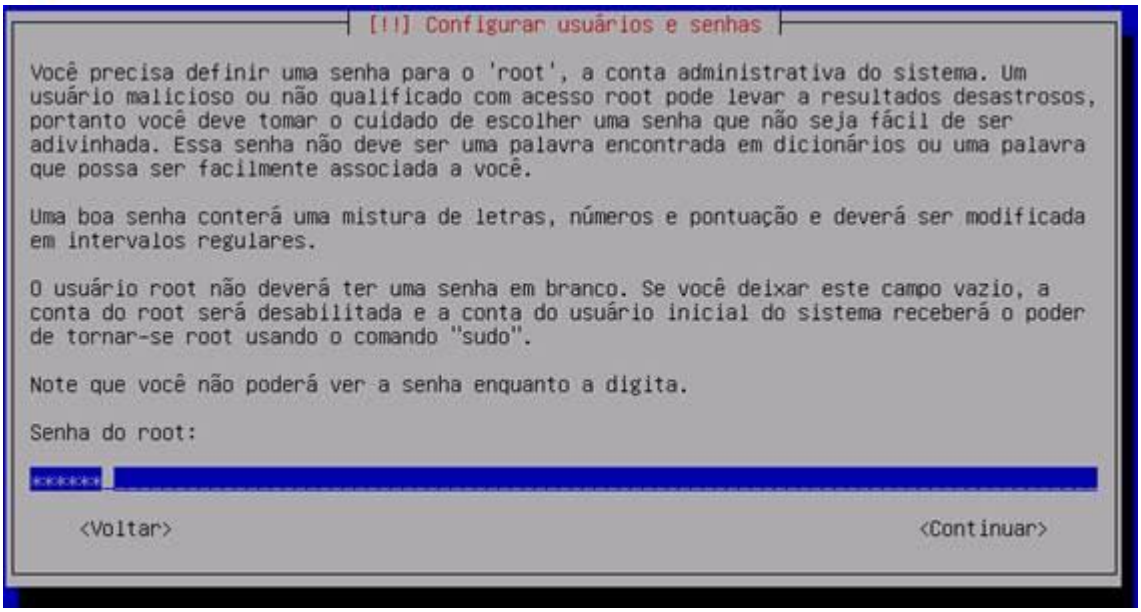

[!!] Configurar usuários e senhas
Você precisa definir uma senha para o 'root', a conta administrativa do sistema. Um usuário malicioso ou não qualificado com acesso root pode levar a resultados desastrosos, portanto você deve tomar o cuidado de escolher uma senha que não seja fácil de ser adivinhada. Essa senha não deve ser uma palavra encontrada em dicionários ou uma palavra que possa ser facilmente associada a você.
Uma boa senha conterá uma mistura de letras, números e pontuação e deverá ser modificada em intervalos regulares.
O usuário root não deverá ter uma senha em branco. Se você deixar este campo vazio, a conta do root será desabilitada e a conta do usuário inicial do sistema receberá o poder de tornar-se root usando o comando "sudo".
Note que você não poderá ver a senha enquanto a digita.
Senha do root:
******
<Voltar>
<Continuar>

Figura 7 - Configurar usuários e senha

Nesta tela o usuário deve definir a senha de Root do sistema, ou seja, a senha de administrador. Ao selecionar a senha de "***root***" pressione a tecla "***Enter***".

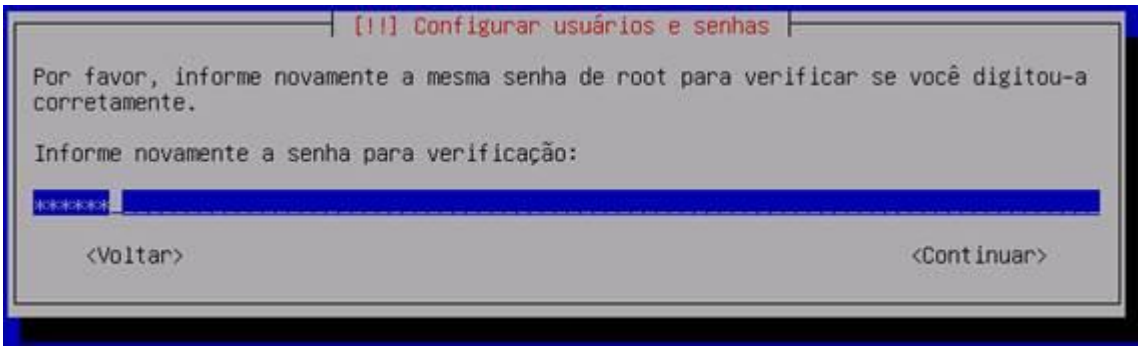

[!!] Configurar usuários e senhas
Por favor, informe novamente a mesma senha de root para verificar se você digitou-a corretamente.
Informe novamente a senha para verificação:
******
<Voltar>
<Continuar>

Figura 8 - confirmação de senha

Confirme a senha de "***root***" e pressione a tecla "***Enter***"

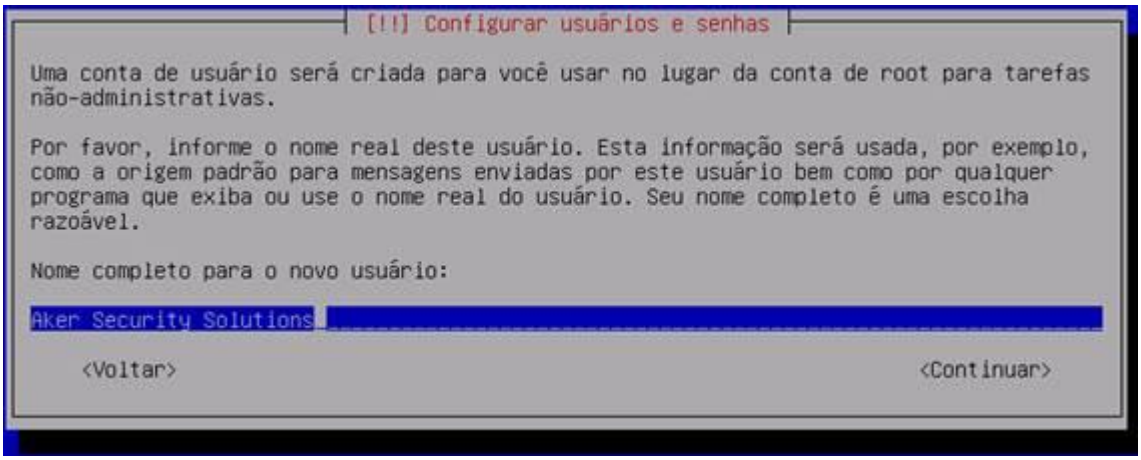

[!!] Configurar usuários e senhas
Uma conta de usuário será criada para você usar no lugar da conta de root para tarefas não-administrativas.
Por favor, informe o nome real deste usuário. Esta informação será usada, por exemplo, como a origem padrão para mensagens enviadas por este usuário bem como por qualquer programa que exiba ou use o nome real do usuário. Seu nome completo é uma escolha razoável.
Nome completo para o novo usuário:
Aker Security Solutions
<Voltar>
<Continuar>

Figura 9 - Nome completo para o novo usuário

Nesta tela o usuário deve definir o nome de usuário para sua conta. Esta conta de usuário será criada para que o usuário possa executar tarefas não administrativas. Tarefas

administrativas podem ser executadas somente com a conta de "***root***" que foi criada anteriormente. Insira o nome desejado e pressione a tecla "***Enter***".

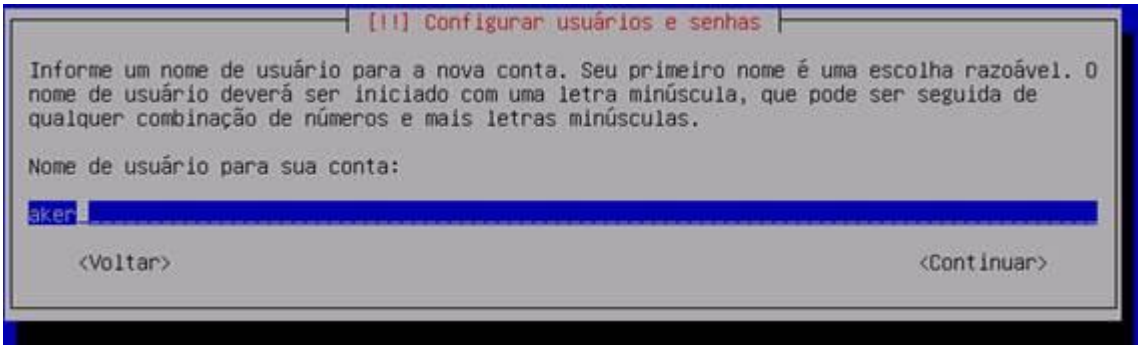

[!!] Configurar usuários e senhas
Informe um nome de usuário para a nova conta. Seu primeiro nome é uma escolha razoável. O nome de usuário deverá ser iniciado com uma letra minúscula, que pode ser seguida de qualquer combinação de números e mais letras minúsculas.
Nome de usuário para sua conta:
aker
<Voltar>
<Continuar>

Figura 10 - Nome de usuário para sua conta

Nesta tela o usuário deve definir o nome de usuário. Ao definir o nome de usuário desejado pressione a tecla "***Enter***".

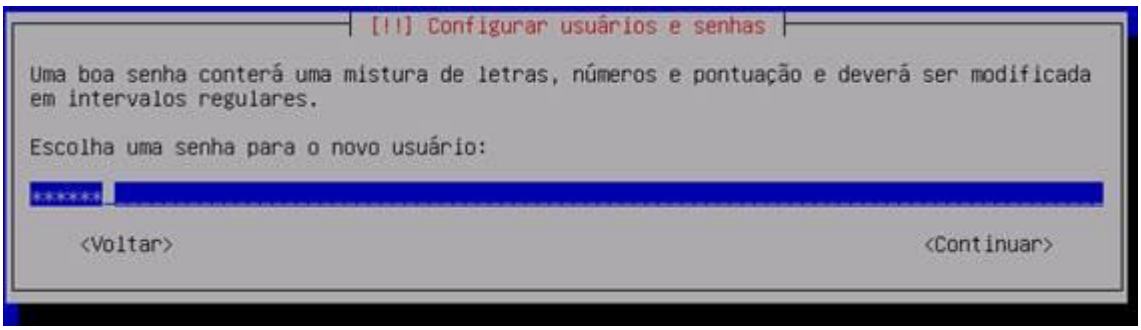

[!!] Configurar usuários e senhas
Uma boa senha conterá uma mistura de letras, números e pontuação e deverá ser modificada em intervalos regulares.
Escolha uma senha para o novo usuário:
******
<Voltar>
<Continuar>

Figura 11 - senha para novo usuário

Nesta tela o usuário deve definir sua senha de usuário. Ao definir a senha desejada pressione a tecla "***Enter***".

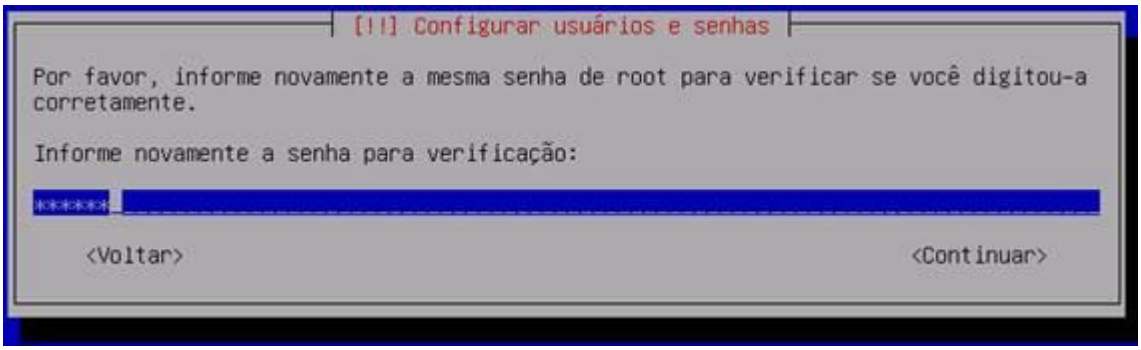

[!!] Configurar usuários e senhas
Por favor, informe novamente a mesma senha de root para verificar se você digitou-a corretamente.
Informe novamente a senha para verificação:
******
<Voltar>
<Continuar>

Figura 12 - confirmação de senha

Confirme a senha de usuário e pressione a tecla "***Enter***"

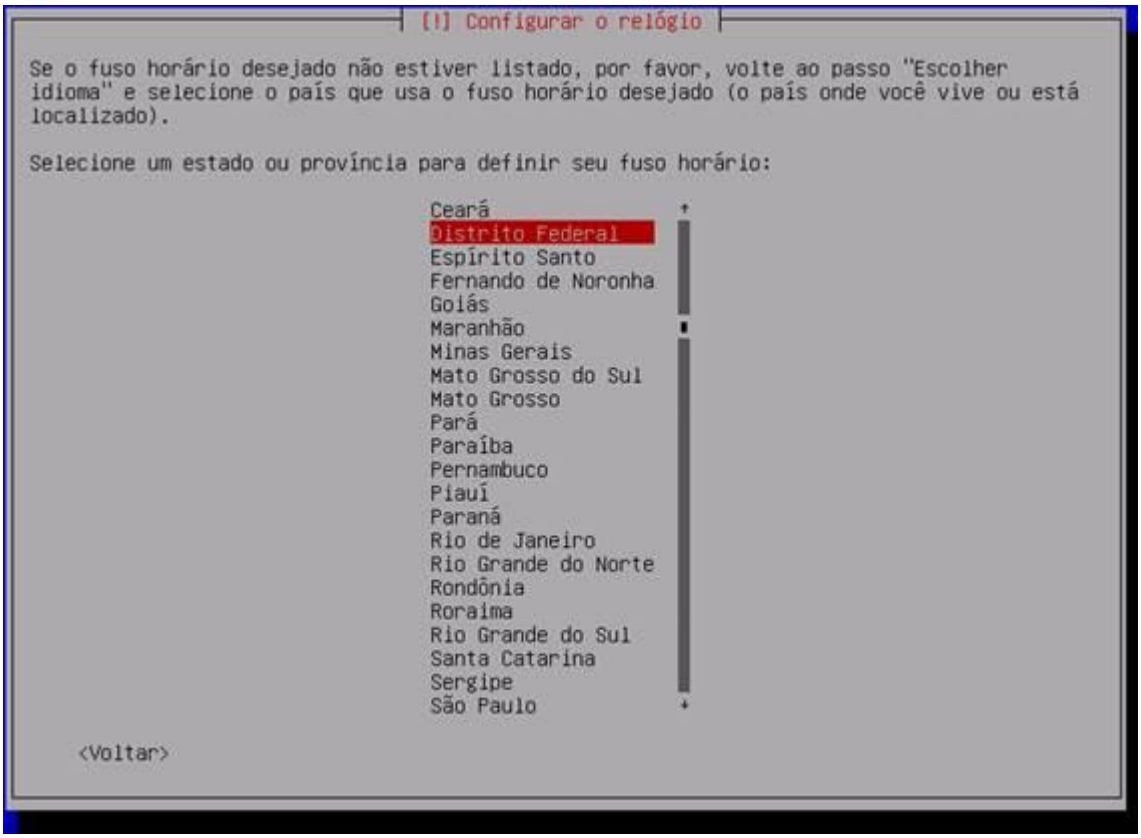


Figura 13 - configuração do relógio

Nesta tela o usuário deve selecionar o estado ou província para definir seu fuso horário. Ao definir sua localidade pressione a tecla "***Enter***".

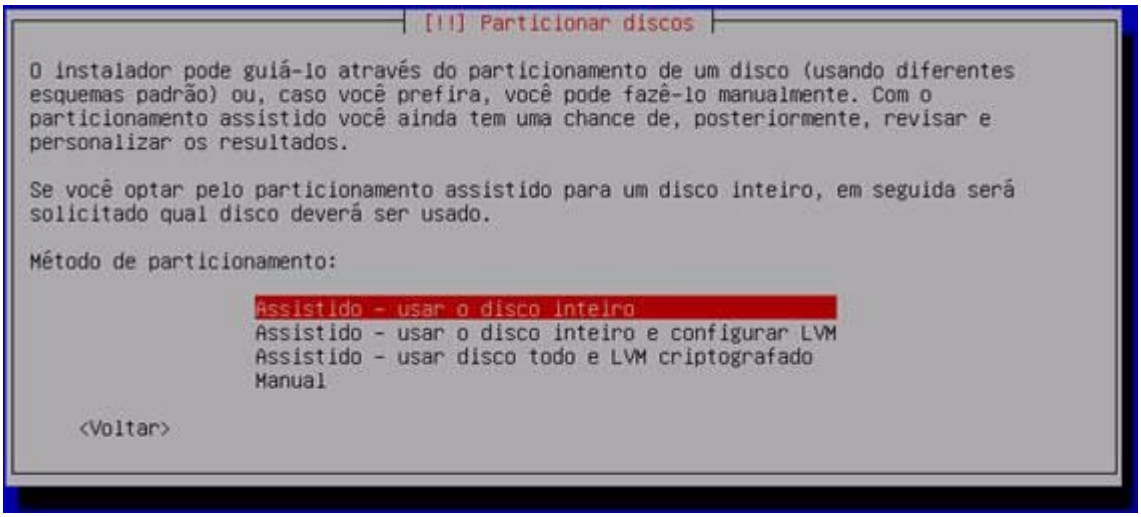

[!!] Particionar discos
O instalador pode guiá-lo através do particionamento de um disco (usando diferentes esquemas padrão) ou, caso você prefira, você pode fazê-lo manualmente. Com o particionamento assistido você ainda tem uma chance de, posteriormente, revisar e personalizar os resultados.
Se você optar pelo particionamento assistido para um disco inteiro, em seguida será solicitado qual disco deverá ser usado.
Método de particionamento:
Assistido - usar o disco inteiro
Assistido - usar o disco inteiro e configurar LVM
Assistido - usar disco todo e LVM criptografado
Manual
<Voltar>

Figura 14 - Particionar discos

Nesta tela o usuário deve selecionar qual método de particionamento que será usado. Selecione o método desejado e clique em "***Continuar***".

É recomendado que o disco seja particionado usando a opção "***Assistido – usar o disco inteiro e configurar LVM***".

O LVM faz com que a administração de partições fique mais flexível oferecendo as seguintes vantagens:

- Redimensionamento de partições em tempo real, ou seja, aumentar o tamanho de partições com o sistema operacional sendo utilizado;
- Junção de várias Partições;
- Junção de vários HDs;
- Criação de imagens de backup;
- Stripping;
- Mirroring;

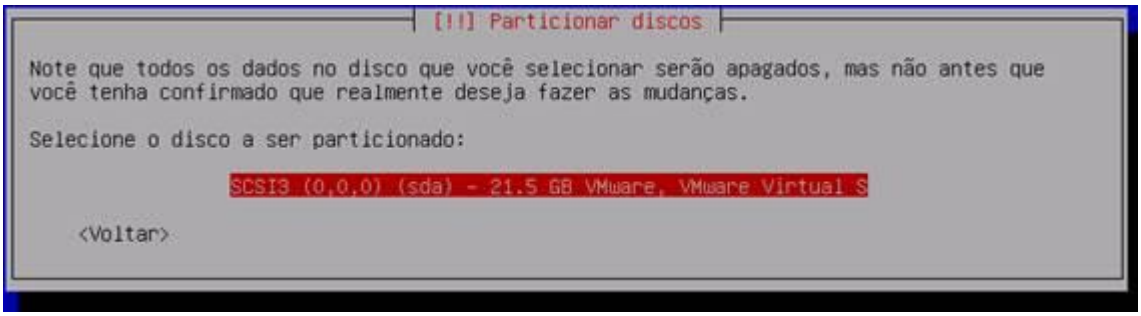

[!!] Particionar discos
Note que todos os dados no disco que você selecionar serão apagados, mas não antes que você tenha confirmado que realmente deseja fazer as mudanças.
Selecione o disco a ser particionado:
SCSI3 (0,0,0) (sda) - 21.5 GB VMware, VMware Virtual S
<Voltar>

Figura 15 - seleção de disco a ser particionado

Selecione o disco a ser particionado e pressione a tecla "***Enter***".

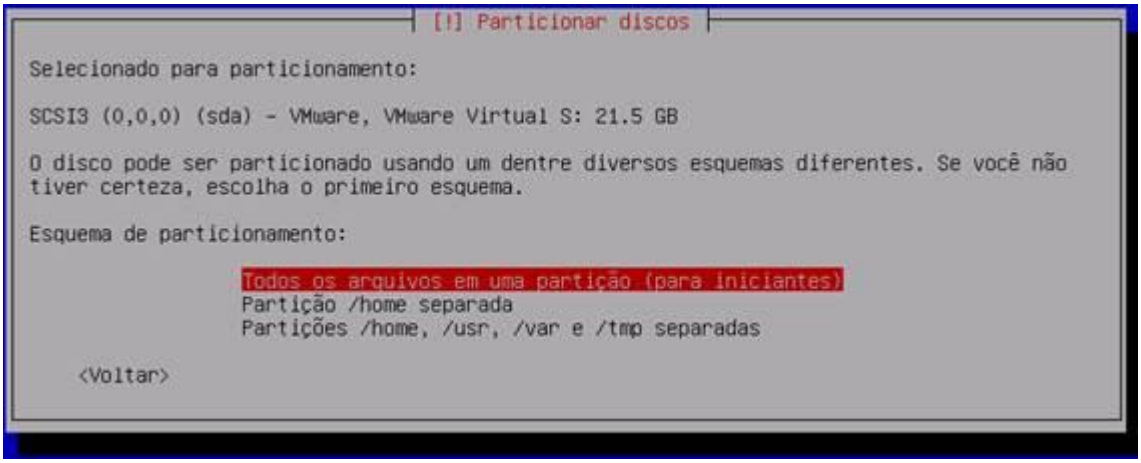

[!] Particionar discos
Selecionado para particionamento:
SCSI3 (0,0,0) (sda) - VMware, VMware Virtual S: 21.5 GB
O disco pode ser particionado usando um dentre diversos esquemas diferentes. Se você não tiver certeza, escolha o primeiro esquema.
Esquema de particionamento:
Todos os arquivos em uma partição (para iniciantes)
Partição /home separada
Partições /home, /usr, /var e /tmp separadas
<Voltar>

Figura 16 - Esquema de particionamento

Nesta tela o usuário deve selecionar qual o esquema de particionamento do sistema. Ao definir o esquema de particionamento desejado pressione a tecla "***Enter***".

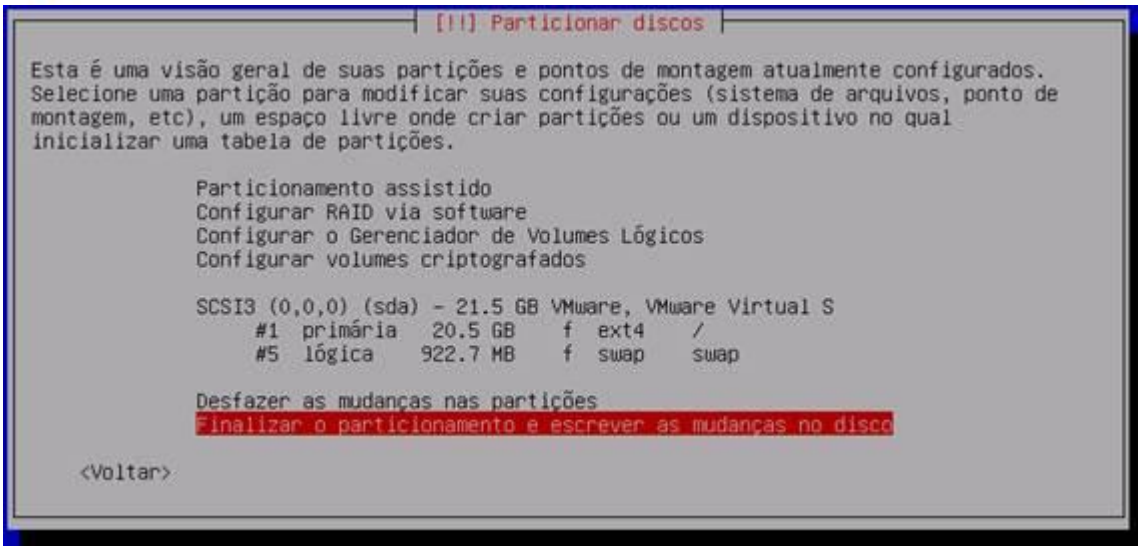

[!!] Particionar discos
Esta é uma visão geral de suas partições e pontos de montagem atualmente configurados.
Selecione uma partição para modificar suas configurações (sistema de arquivos, ponto de
montagem, etc), um espaço livre onde criar partições ou um dispositivo no qual
inicializar uma tabela de partições.
Particionamento assistido
Configurar RAID via software
Configurar o Gerenciador de Volumes Lógicos
Configurar volumes criptografados
SCSI3 (0,0,0) (sda) - 21.5 GB VMware, VMware Virtual S
#1 primária 20.5 GB f ext4 /
#5 lógica 922.7 MB f swap swap
Desfazer as mudanças nas partições
Finalizar o particionamento e escrever as mudanças no disco
<Voltar>

Figura 17 - Finalizar o particionamento e escrever as mudanças no disco

Esta tela exibe as configurações da partição de disco. Ao verificar as informações selecione a opção "***Finalizar o particionamento e escrever as mudanças no disco***" pressione a tecla "***Enter***".

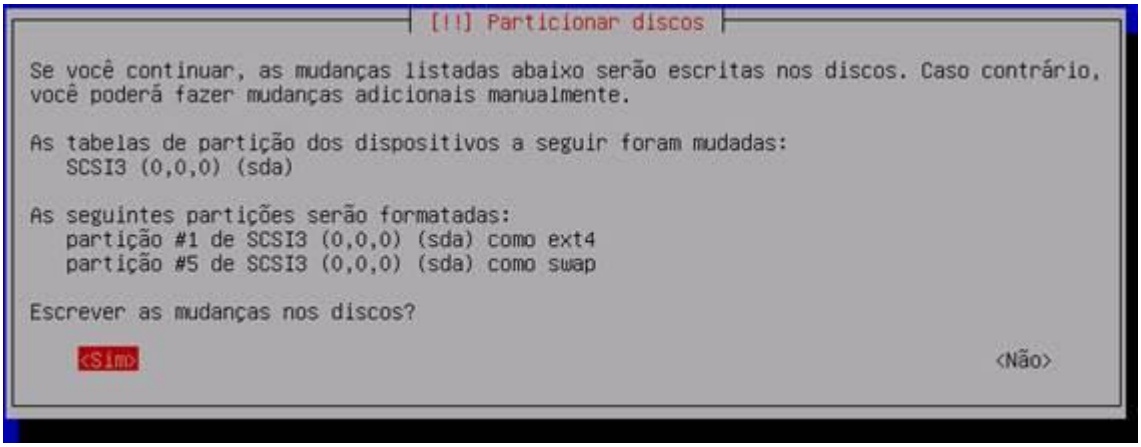

[!!] Particionar discos
Se você continuar, as mudanças listadas abaixo serão escritas nos discos. Caso contrário,
você poderá fazer mudanças adicionais manualmente.
As tabelas de partição dos dispositivos a seguir foram mudadas:
SCSI3 (0,0,0) (sda)
As seguintes partições serão formatadas:
partição #1 de SCSI3 (0,0,0) (sda) como ext4
partição #5 de SCSI3 (0,0,0) (sda) como swap
Escrever as mudanças nos discos?
<Sim>
<Não>

Figura 18 - Confirmação e mudanças

Nesta tela o usuário deve confirmar se as mudanças exibidas serão ou não escritas no disco. Selecione a opção desejada e pressione a tecla "***Enter***".

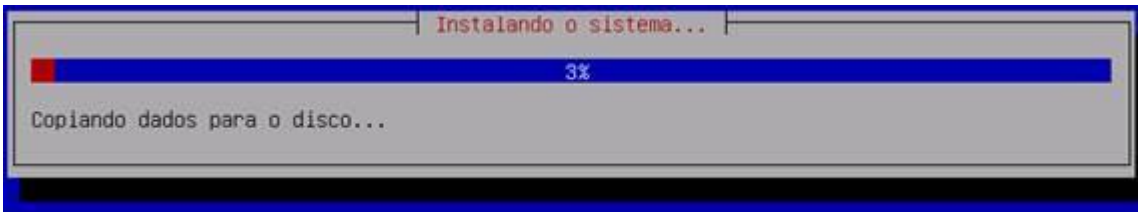


Figura 19 - instalando o sistema

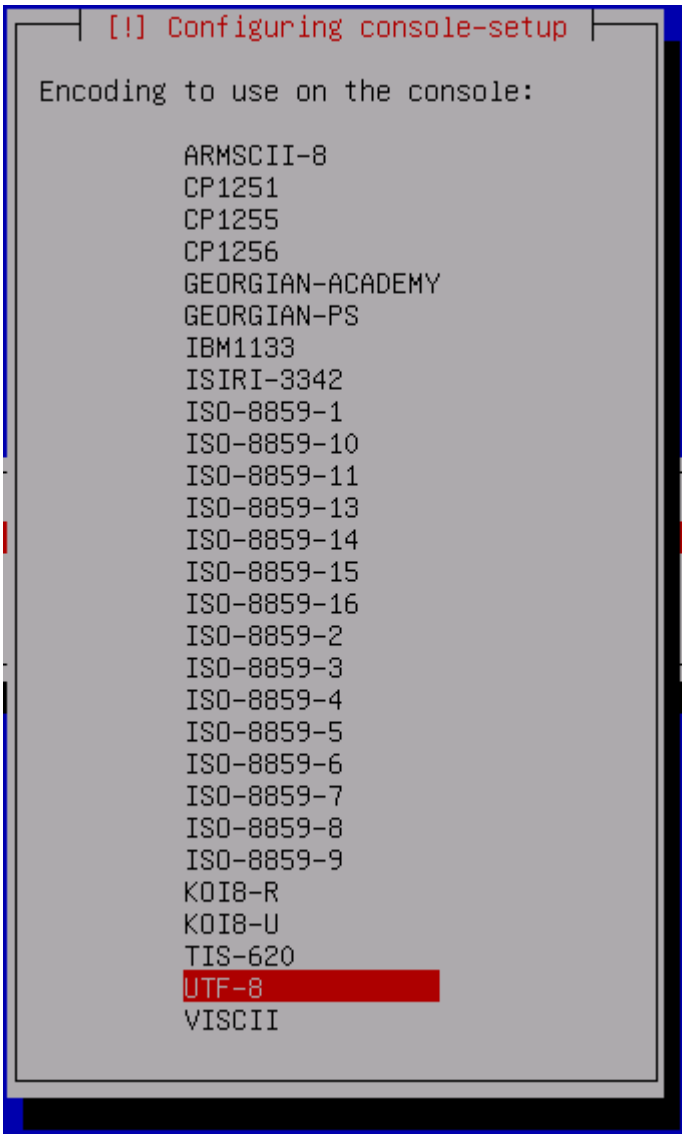


Figura 20 - Método de codificação do console

Nesta tela o usuário deve selecionar o método de codificação do console. Selecione a opção ***UTF-8*** e pressione a tecla "***Enter***".

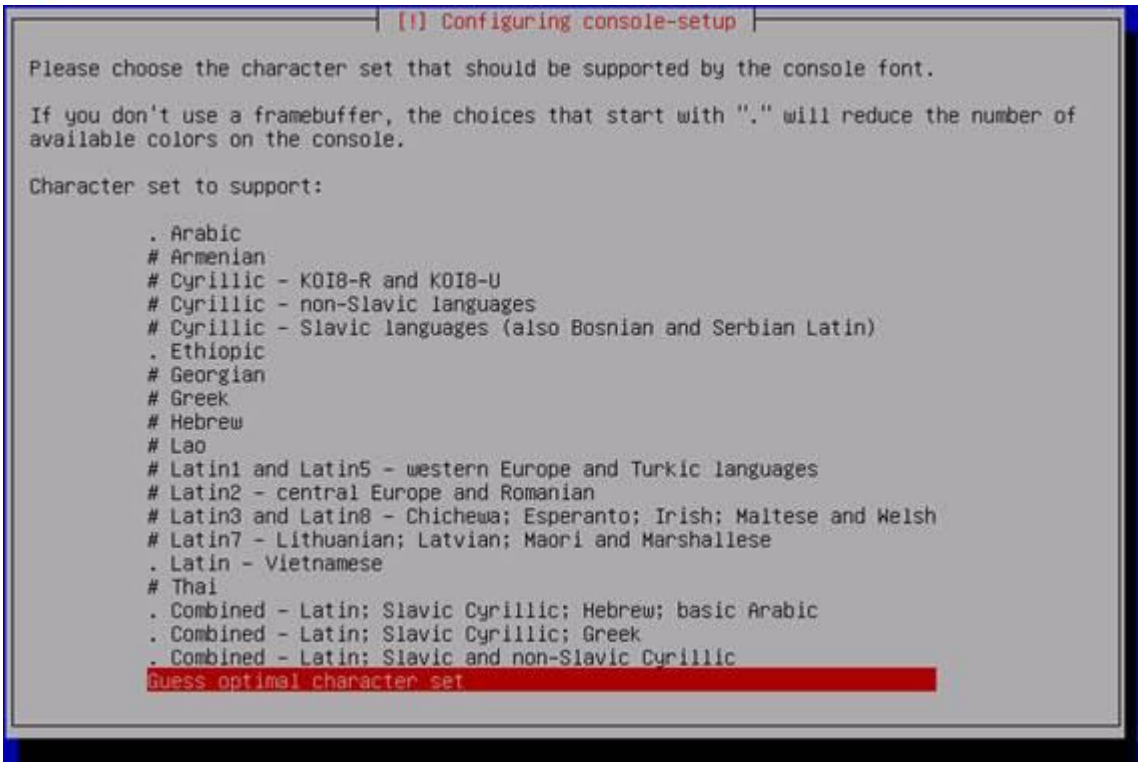

[!] Configuring console-setup
Please choose the character set that should be supported by the console font.
If you don't use a framebuffer, the choices that start with "." will reduce the number of available colors on the console.
Character set to support:
. Arabic
Armenian
Cyrillic - KOI8-R and KOI8-U
Cyrillic - non-Slavic languages
Cyrillic - Slavic languages (also Bosnian and Serbian Latin)
. Ethiopic
Georgian
Greek
Hebrew
Lao
Latin1 and Latin5 - western Europe and Turkic languages
Latin2 - central Europe and Romanian
Latin3 and Latin8 - Chichewa; Esperanto; Irish; Maltese and Welsh
Latin7 - Lithuanian; Latvian; Maori and Marshallese
. Latin - Vietnamese
Thai
. Combined - Latin; Slavic Cyrillic; Hebrew; basic Arabic
. Combined - Latin; Slavic Cyrillic; Greek
. Combined - Latin; Slavic and non-Slavic Cyrillic
Guess optimal character set

Figura 21 - seleção de conjunto de caracteres

Nesta tela o usuário deve selecionar o conjunto de caracteres que será suportado pela fonte do console. Seleciona a opção "***Guess optimal character set***" e pressione a tecla "***Enter***".

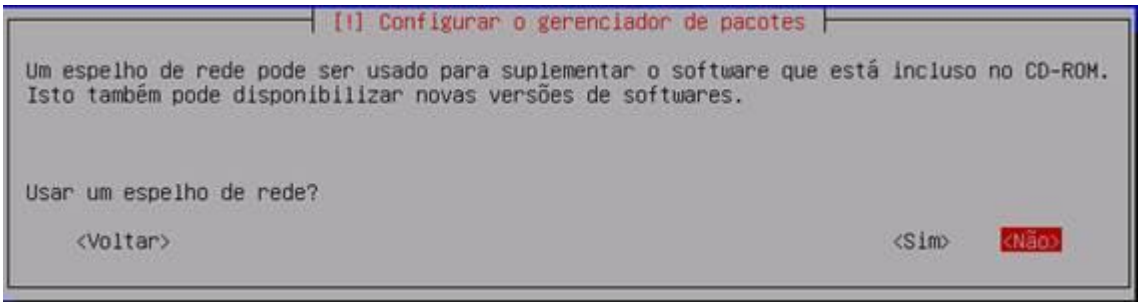

[!] Configurar o gerenciador de pacotes
Um espelho de rede pode ser usado para suplementar o software que está incluso no CD-ROM.
Isto também pode disponibilizar novas versões de softwares.
Usar um espelho de rede?
<Voltar>
<Sim>
<Não>

Figura 22 - configurar o gerenciador de pacotes

Nesta tela o usuário deve selecionar se vai ou não *usar* um espelho de rede. Selecione a opção desejada e pressione a tecla "***Enter***".

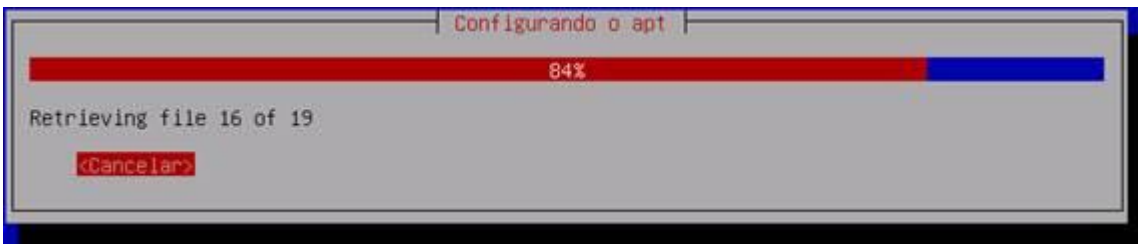


Figura 23 - configurando o apt

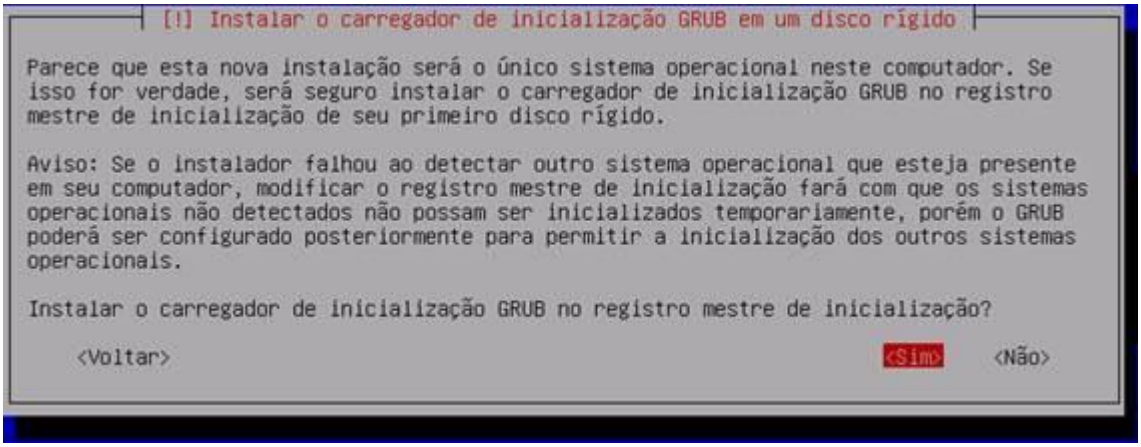

[!] Instalar o carregador de inicialização GRUB em um disco rígido
Parece que esta nova instalação será o único sistema operacional neste computador. Se isso for verdade, será seguro instalar o carregador de inicialização GRUB no registro mestre de inicialização de seu primeiro disco rígido.
Aviso: Se o instalador falhou ao detectar outro sistema operacional que esteja presente em seu computador, modificar o registro mestre de inicialização fará com que os sistemas operacionais não detectados não possam ser inicializados temporariamente, porém o GRUB poderá ser configurado posteriormente para permitir a inicialização dos outros sistemas operacionais.
Instalar o carregador de inicialização GRUB no registro mestre de inicialização?
<Voltar>
<Sim>
<Não>

Figura 24 - instalar o carregador de inicialização GRUB

Nesta tela o usuário deve selecionar a opção "***Sim***" para que o carregador de inicialização GRUB seja instalado no registro mestre de inicialização.

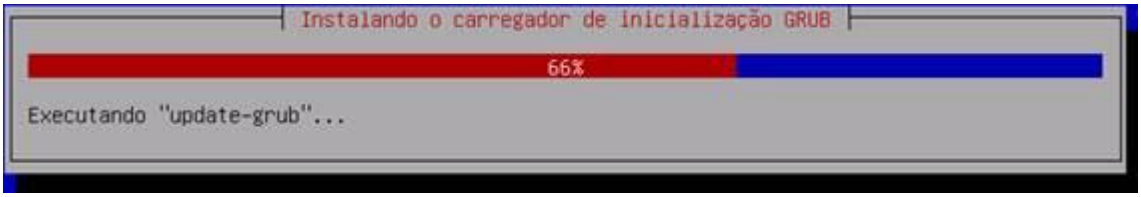


Figura 25 - Instalando o carregador de inicialização GRUB

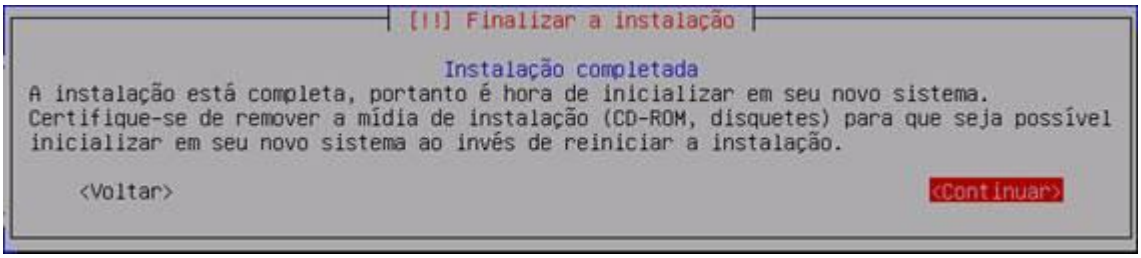

[!!] Finalizar a instalação
Instalação completada
A instalação está completa, portanto é hora de inicializar em seu novo sistema.
Certifique-se de remover a mídia de instalação (CD-ROM, disquetes) para que seja possível inicializar em seu novo sistema ao invés de reiniciar a instalação.
<Voltar>
<Continuar>

Figura 26 - Finalizar a instalação

Esta tela será exibida quando a instalação for concluída. Pressione a tecla "**Enter**" para reiniciar a instalação e iniciar seu novo sistema.

Para visualizar qual o IP que foi designado ao seu Aker Report Center, acesse a Interface de texto, e entre com o comando "***ifconfig***", como exibido na imagem abaixo (Para executar essa operação é necessário estar logado como usuário root):

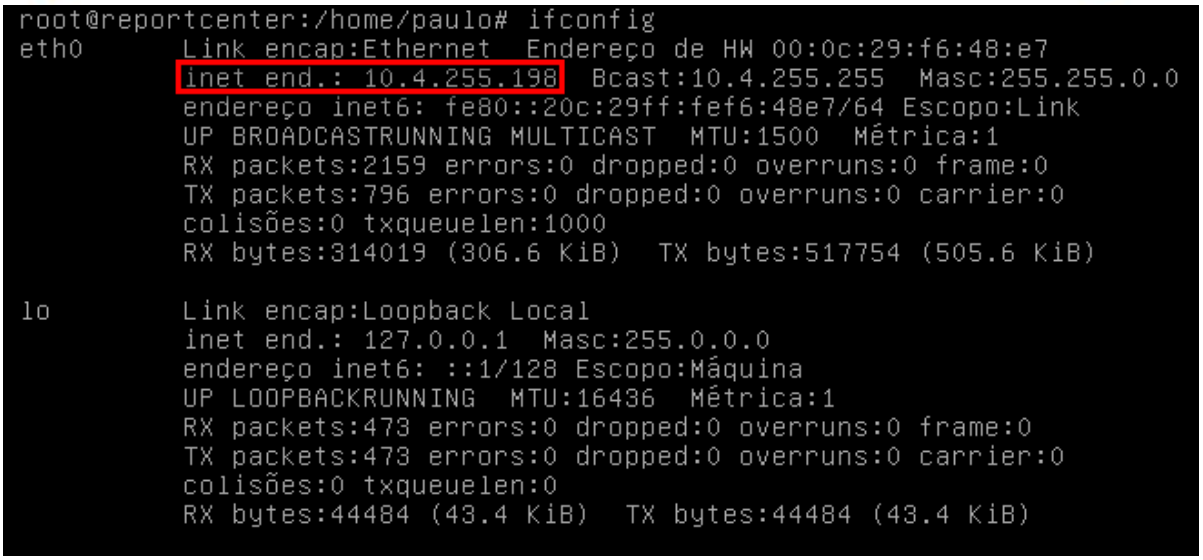

root@reportcenter:/home/paulo# ifconfig
eth0 Link encap:Ethernet Endereço de HW 00:0c:29:f6:48:e7
inet end.: 10.4.255.198 Bcast:10.4.255.255 Masc:255.255.0.0
endereço inet6: fe80::20c:29ff:fef6:48e7/64 Escopo:Link
UP BROADCASTRUNNING MULTICAST MTU:1500 Métrica:1
RX packets:2159 errors:0 dropped:0 overruns:0 frame:0
TX packets:796 errors:0 dropped:0 overruns:0 carrier:0
colisões:0 txqueuelen:1000
RX bytes:314019 (306.6 KiB) TX bytes:517754 (505.6 KiB)
lo Link encap:Loopback Local
inet end.: 127.0.0.1 Masc:255.0.0.0
endereço inet6: ::1/128 Escopo:Máquina
UP LOOPBACKRUNNING MTU:16436 Métrica:1
RX packets:473 errors:0 dropped:0 overruns:0 frame:0
TX packets:473 errors:0 dropped:0 overruns:0 carrier:0
colisões:0 txqueuelen:0
RX bytes:44484 (43.4 KiB) TX bytes:44484 (43.4 KiB)

Figura 27 - Visualizando IP para acesso no browser

Utilize o IP encontrado para fazer o primeiro acesso ao *Aker Report Center* por meio de um browser. O usuário será direcionado para uma tela de configuração que vai finalizar a instalação do sistema.

2.2 Adicionando espaço em disco – LVM

Após adquirir mais espaço em disco, é necessário fazer seu sistema reconhecer o espaço adicional, para isso siga os passos abaixo:

Passo 1

- Acesse seu servidor via SSH, digite seu nome de usuário e senha e execute a sequência de comandos abaixo:

- **# fdisk -l /dev/sda**

1. Anote o valor do último número do cilindro da partição /dev/sda5. ***41940991 no exemplo abaixo***.

```
login as: aker
aker@10.4.255.243's password:
Linux reportcenter 3.2.0-4-amd64 #1 SMP Debian 3.2.57-3 x86_64

Bem vindo ao Aker Report Center!


Last login: Thu Sep 25 13:11:02 2014
aker@reportcenter:~$ su
Senha:
root@reportcenter:/home/aker# fdisk -l /dev/sda

Disk /dev/sda: 53.7 GB, 53687091200 bytes
255 heads, 63 sectors/track, 6527 cylinders, total 104857600 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000dc9de

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048      499711      248832   83  Linux
/dev/sda2          501758    41940991    20719617    5  Extended
/dev/sda5          501760    41940991    20719616   8e  Linux LVM
```

Figura 28 - comando fdisk -l /dev/sda

Em seguida entre com o comando, abaixo é pressione a tecla 'Enter':

- **# fdisk /dev/sda**

2. Na linha abaixo digite '**N**', para inserir uma nova partição.

```
root@reportcenter:/home/aker# fdisk /dev/sda

Command (m for help): n
```

Figura 29 - digite 'N' para inseir uma nova partição

3. Na linha abaixo digite '**P**' e pressione a tecla "Enter", para adicionar uma partição primária.

```
root@reportcenter:/home/aker# fdisk /dev/sda

Command (m for help): n
Partition type:
   p   primary (1 primary, 1 extended, 2 free)
   l   logical (numbered from 5)
Select (default p): p
```

Figura 30 - digite 'p' para adicionar uma partição primária

4. Em número da partição (partition number), digite 3 e pressione a tecla "Enter";

```
Partition number (1-4, default 3): 3
First sector (499712-104857599, default 499712):
```

Figura 31 - definindo o número da partição

5. Digite o número que foi anotou primeira imagem para que o cilindro se inicie a partir dele.

```
First sector (499712-104857599, default 499712): 41940991
Sector 41940991 is already allocated
```

Figura 32 - definindo o valor para o primeiro setor

6. Para o resto do cilindro ele vai te mostra todo o espaço disponível, apenas pressione a tecla "Enter".

```
First sector (499712-104857599, default 499712): 41940991
Sector 41940991 is already allocated
First sector (41940992-104857599, default 41940992):
Using default value 41940992
Last sector, +sectors or +size{K,M,G} (41940992-104857599, default 104857599):
```

Figura 33 - Informação dos setores

7. Digite '**P**' para visualizar a nova partição criada, **/dev/sda3**

```
   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048      499711      248832   83  Linux
/dev/sda2          501758    41940991    20719617    5  Extended
/dev/sda3        41940992   104857599    31458304   83  Linux
/dev/sda5          501760    41940991    20719616   8e  Linux LVM
```

Figura 34 - Visualizando a nova partição

8. Digite '**W'** para salvar e aplicar as alterações no disco;

Uma mensagem de "**WARNING**" será exibida, informando que as alterações serão aplicadas somente após a reinicialização.

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Dispositivo ou recurso estÃ; ocupado.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
```

Figura 35 - mensagem de Warning

9. Em seguida reinicie o servidor com o comando '**reboot**' para que o sistema reconheça as novas partições;

```
root@reportcenter:/home/aker# reboot

The system is going down for reboot NOW! (pts/0) (Thu Sep 25 17:24:51 2014):
root@reportcenter:/home/aker#
```

Figura 36 – Reiniando a maquina para aplicar as mudanças

Passo 2

Após reiniciar o servidor, será necessário adicionar as partições ao LVM, para isso execute os comandos abaixo:

1. Crie a nova partição no LVM executando o comando abaixo;

```
root@reportcenter:/home/aker# pvcreate /dev/sda3
  Writing physical volume data to disk "/dev/sda3"
  Physical volume "/dev/sda3" successfully created
root@reportcenter:/home/aker#
```

Figura 37 - comando para cria uma nova partição no LVM

2. Agora, deve-se expandir o *Volume do reportcenter* adicionando o sda3, para isso use o comando abaixo;

```
root@reportcenter:/home/aker# vgextend reportcenter /dev/sda3
  Volume group "reportcenter" successfully extended
root@reportcenter:/home/aker#
```

Figura 38 - comando para expandir o volume do reportcenter

3. Estendemos o volume lógico da LVM com o valor contratado a mais;

```
root@reportcenter:/home/aker# lvextend -l +100%FREE /dev/reportcenter/root
  Extending logical volume root to 49,01 GiB
  Logical volume root successfully resized
root@reportcenter:/home/aker#
```

Figura 39 - comando para expandir o volume lógico da LVM

Assumindo que o VG se chama reportcenter e o volume lógico a ser expandido se chama root, o **-l +100%FREE** deve ser usado para usar todo o espaço disponível para expansão.

4. Use o comando abaixo para redimensionar o sistema de arquivos da partição /reportcenter/root;

```
root@reportcenter:/home/aker# resize2fs /dev/reportcenter/root
resize2fs 1.42.5 (29-Jul-2012)
Filesystem at /dev/reportcenter/root is mounted on /; on-line resizing required
old_desc_blocks = 2, new_desc_blocks = 4
Performing an on-line resize of /dev/reportcenter/root to 12847104 (4k) blocks.
The filesystem on /dev/reportcenter/root is now 12847104 blocks long.
```

Figura 40 - comando para redimensionar o sistema de arquivos

5. Reinicie o servidor novamente para finalizar o processo;

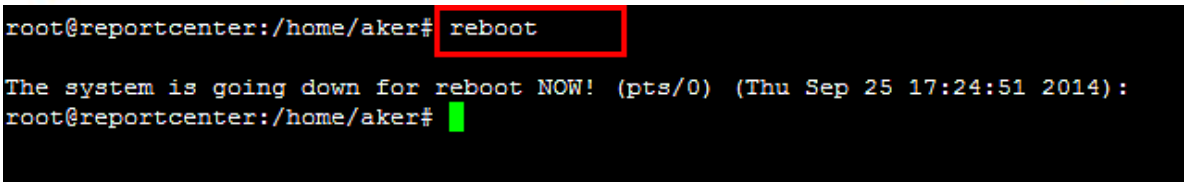

root@reportcenter:/home/aker# reboot
The system is going down for reboot NOW! (pts/0) (Thu Sep 25 17:24:51 2014):
root@reportcenter:/home/aker#

Figura 41 - reiniciar o sistema para aplicar as alterações

Ao reiniciar, o espaço expandido no disco será reconhecido e já poderá ser utilizado.

2.3 *Assistente de Configuração do Aker Report Center*

No primeiro acesso ao *Aker Report Center* por meio de um browser, o usuário será direcionado para a tela do Assistente de Configuração do *Aker Report Center*, que irá definir senha do banco de dados, usuário administrador do sistema e finalizar instalação.

Informações Gerais

Esta tela informa que o Aker Report Center foi instalado com sucesso, e fornece acesso ao Manual do produto, e acesso ao Fórum da Aker.

Clique em "***Próximo***" para continuar com a configuração:

Aker Report Center
Informações Gerais
Banco de Dados
Informações do Administrador
Finalizando a Instalação
Prezado (a) usuário (a),
O Aker Report Center foi instalado com sucesso. Precisamos apenas configurar alguns itens, antes que você comece a utilizar o sistema. Para isso, navegue pelas abas acima ou por meio da paginação abaixo e preencha as informações necessárias.
Em caso de dúvidas, consulte o Manual do Aker Report Center ou acesse o Aker Fórum.
Anterior
Próximo

Figura 42 - Informações Gerais

Banco de Dados

Nesta janela o usuário deve criar uma senha para a autenticação do sistema com o banco de dados de configuração.

Figura 43 - Banco de dados

Informações do Administrador

Nesta janela o usuário deve configurar a conta de administrador do sistema, informando login, e senha. Caso opte por não configurar os campos serão definidos pelo padrão do sistema:

- ***Senha padrão Interface texto***

Usuário padrão SSH: aker

Senha padrão SSH: 123456

- ***Senha padrão Interface remota***

Usuário padrão: admin

Senha padrão: 123456

Figura 44 - Informações do Administrador

Finalizando a Instalação

Esta tela informa ao usuário que as informações necessárias para a configuração foram fornecidas e a configuração pode ser iniciada. Para prosseguir com a Instalação clique em "*Instalar*", e para revisar as informações fornecidas clique em "*Anterior*".

Aker Report Center
Informações Gerais
Banco de Dados
Informações do Administrador
Finalizando a Instalação
Quase pronto! Confira as informações preenchidas anteriormente e clique no botão "Instalar" para concluirmos a sua instalação.
Anterior
Instalar

Figura 45 - Finalizando a Instalação

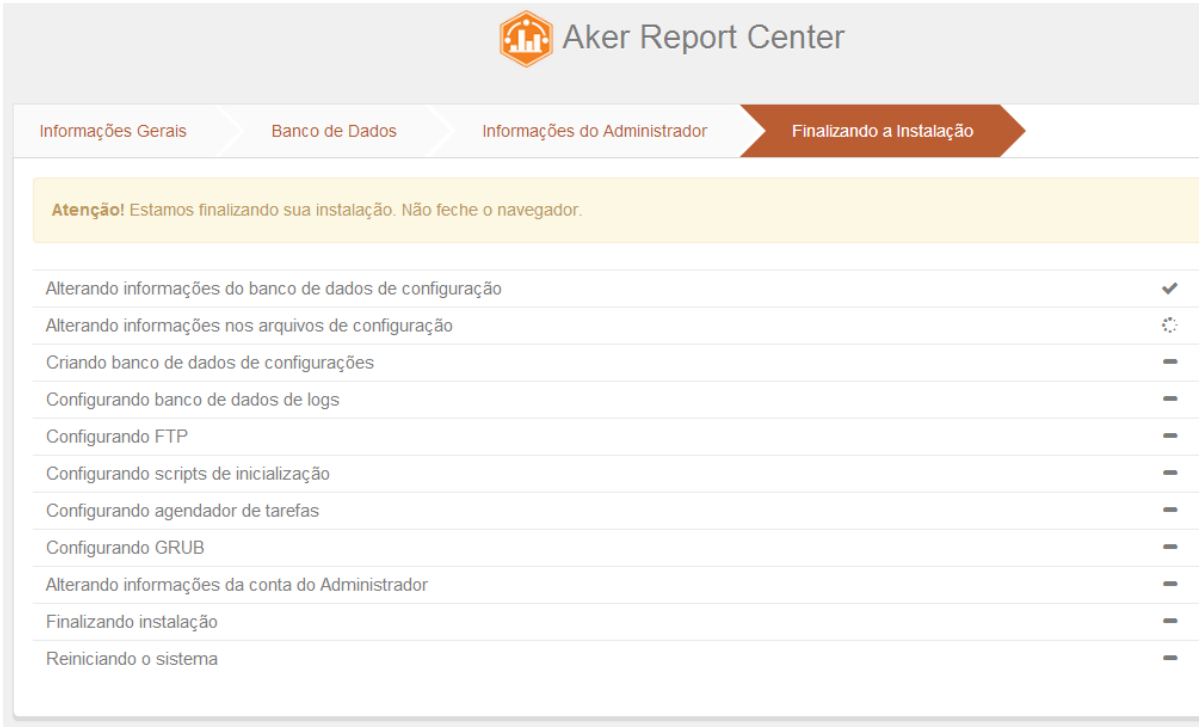

Aker Report Center
Informações Gerais
Banco de Dados
Informações do Administrador
Finalizando a Instalação
Atenção! Estamos finalizando sua instalação. Não feche o navegador.
Alterando informações do banco de dados de configuração
Alterando informações nos arquivos de configuração
Criando banco de dados de configurações
Configurando banco de dados de logs
Configurando FTP
Configurando scripts de inicialização
Configurando agendador de tarefas
Configurando GRUB
Alterando informações da conta do Administrador
Finalizando instalação
Reiniciando o sistema

Figura 46 - Finalizando os processos

Ao concluir a instalação é necessário que o usuário aguarde a reinicialização do sistema, que irá redireciona-lo para a tela de login do *Aker Report Center*.

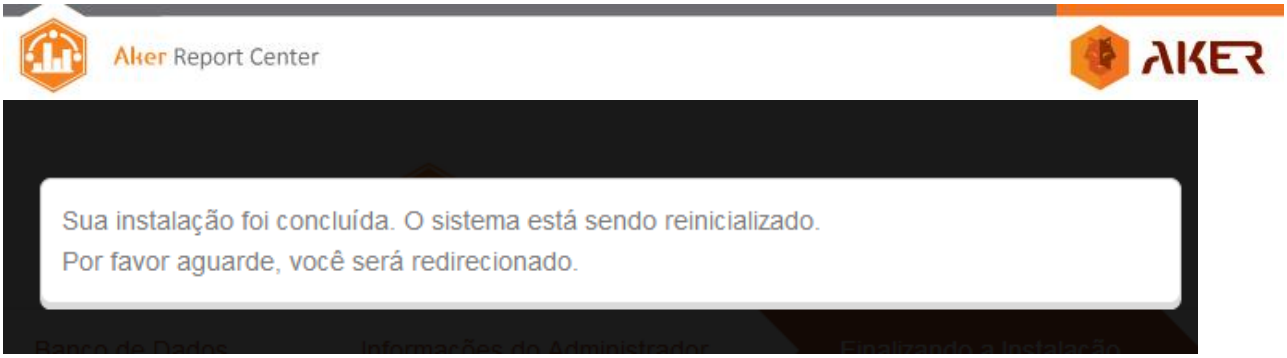

Aker Report Center
AKER
Sua instalação foi concluída. O sistema está sendo reinicializado.
Por favor aguarde, você será redirecionado.

Figura 47 - Mensagem de reinicialização do sistema

2.4 Licenciamento

Ao terminar a instalação do sistema, o usuário deve acessar o endereço que é previamente configurado no **modo SSH – Interface texto** (a *interface de rede é configurada por padrão em modo DHCP*) e entrar com o nome de usuário e senha. A seguir as senhas padrões do Aker Report Center.

- ***Senha padrão Interface texto***

Usuário padrão SSH: aker

Senha padrão SSH: 123456

- ***Senha padrão Interface remota***

Usuário padrão: admin

Senha padrão: 123456

O número máximo de tentativas para logar-se no ***Aker report Center*** são 3, caso o usuário exceda o número máximo de tentativas o mesmo deverá esperar 2 minutos para tentar efetuar o login novamente.

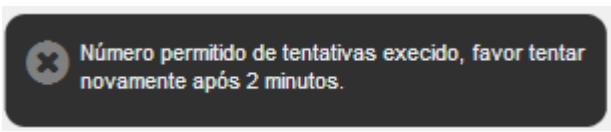


Figura 48 - Mensagem ao errar a senha mais de 3 vezes

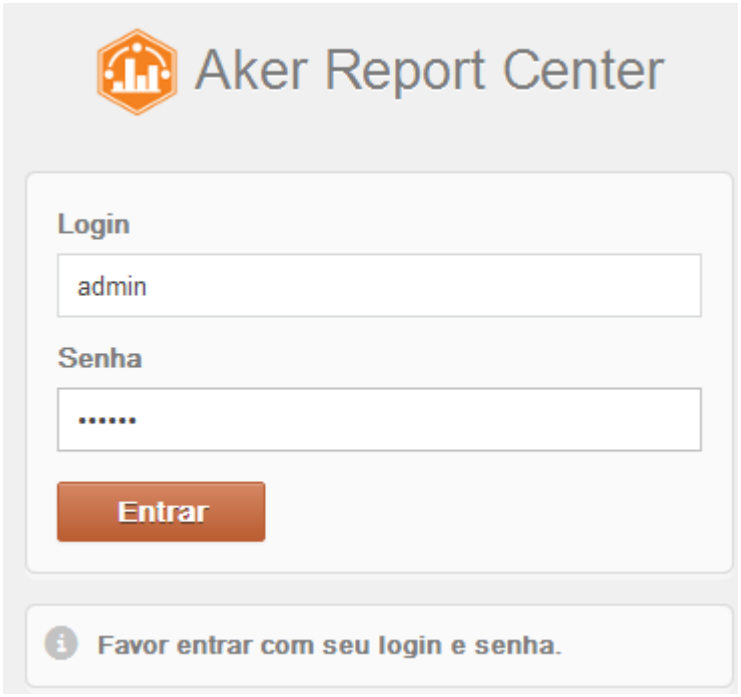


Figura 49 - Tela de login

No primeiro login o usuário deve gerar a chave de licenciamento do produto. Ao gerar a chave de licenciamento o usuário deve enviar a mesma para licenca@aker.com.br solicitando sua licença.

Para gerar a chave de licenciamento do produto e carregar a licença do produto siga os passos abaixo:

- Preencha os dados da janela abaixo corretamente e clique em

.

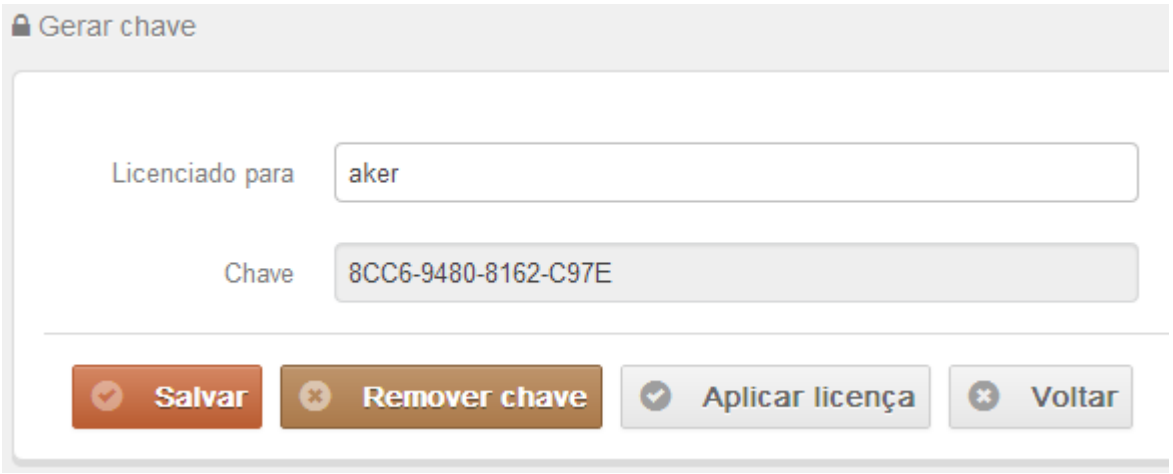


Figura 50 - Gerar chave

Licenciando para: Neste campo deve-se informar o nome do usuário ou empresa para qual o produto está sendo licenciado.

O nome usado na opção "***Licenciando para***" deve ser o mesmo usado no AGL.

Chave: Ao preencher o campo acima e clicar em "***Salvar***" fará com que a chave de licenciamento seja gerada automaticamente, o usuário deve encaminha está chave para licenca@aker.com.br solicitando sua licença, ao receber a licença siga os passos a seguir (*ao enviar a solicitação o usuário receberá sua licença no período máximo de 24h*).

- Ao receber a licença clique em

- Na janela Aplicar Licença clique no ícone para localizar sua licença.

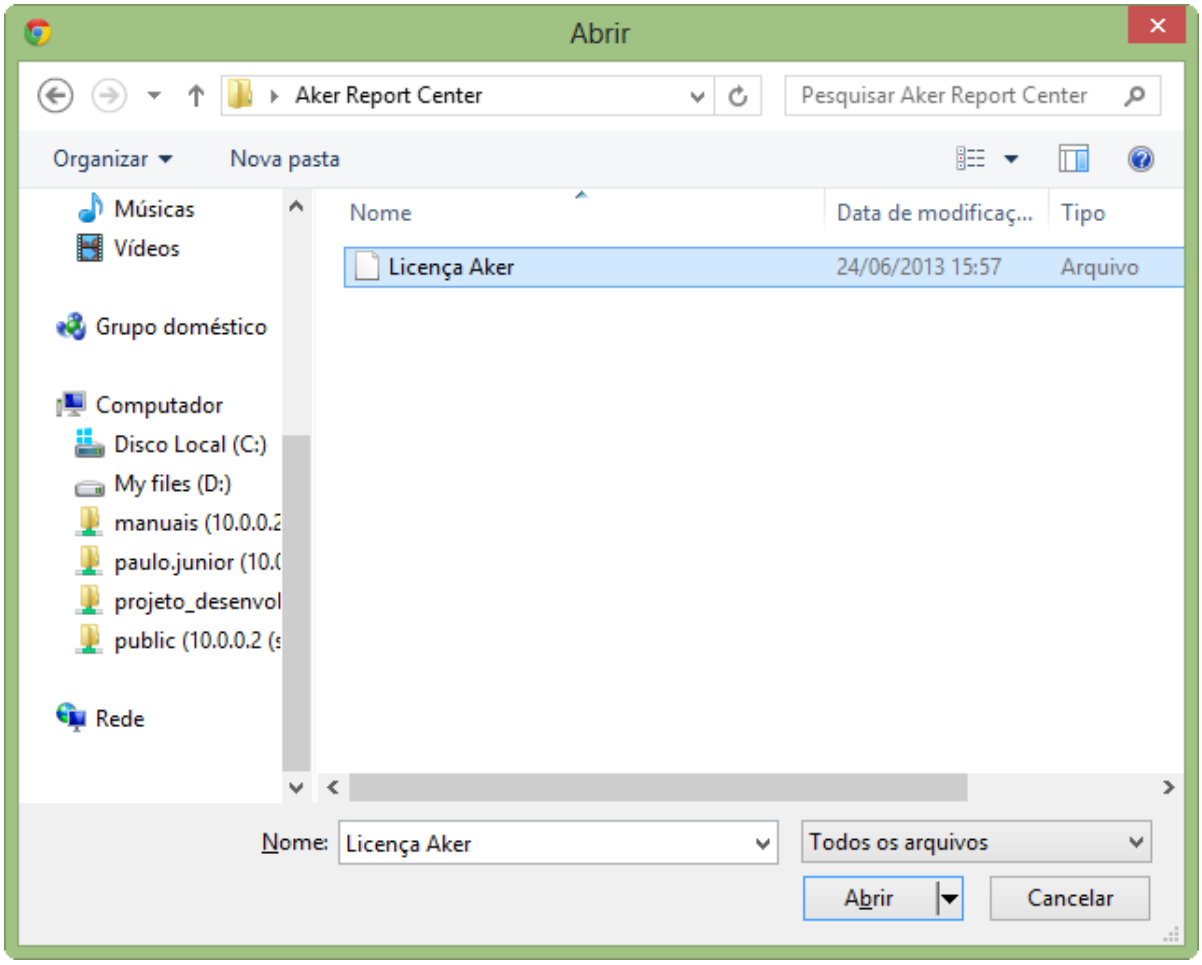


Figura 51 - Localizando lincença

Figura 52 - Opções de carregamento da licença

- Ao localizar o arquivo clique em para carregar o arquivo. Ao carregar a licença suas informações serão exibidas na mesma tela como na imagem a seguir:

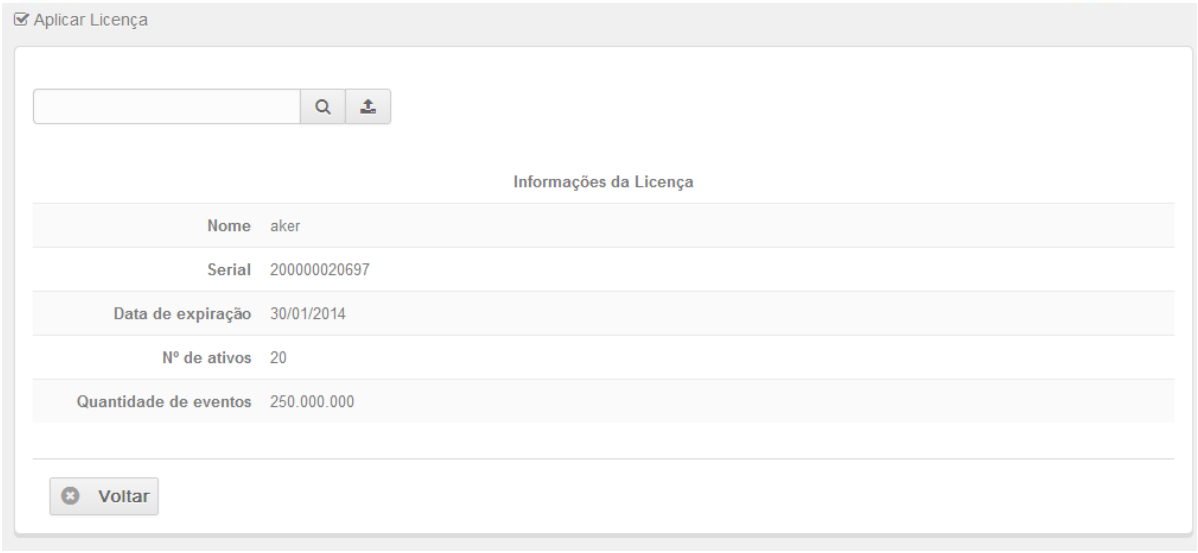


Figura 53 - Informação da licença

Após carregar a licença, serão exibidas as informações sobre sua licença:

Nome: Neste campo é exibido o nome do titular da licença;

Serial: Neste campo é exibido o serial da licença em uso/carregada;

Data de expiração: Neste campo é exibida a data de expiração da licença em uso/carregada;

N° de ativos: Neste campo é exibido o número de ativos suportados pela licença em uso/carregada ativo para a licença em questão;

Quantidades de eventos: Neste campo é exibida a quantidade de eventos suportada pela licença em uso/carregada;

Esta janela permite que o usuário visualize as informações de usa licença em uso, lembrando que ao carregar uma nova licença as informações serão atualizadas mostrando assim as informações da nova licença que foi carregada.

Depois de completar o processo de upload da licença no sistema, serão exibidas as informações da licença, clique no botão

depois do upload para completar processo de licenciamento.

O sistema enviará mensagens automáticas de notificação para o cliente quando o número máximo de eventos suportado pela licença em questão estiver próximo de ser atingido. Quando a licença se expirar o Aker Report Center não irá gerar relatórios, mas todos os logs recebidos são armazenados, e uma vez que a licença for regularizada os logs armazenados serão tratados e o usuário poderá gerar relatórios com estes logs.

O Aker Report Center possui quatro menus principais que facilitam o gerenciamento do administrator. Estes menus serão abordados nos capítulos a seguir.

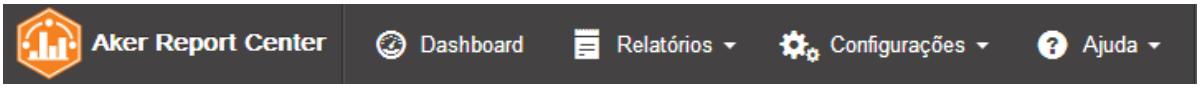


Figura 54 - Menus

Dashboard

3 Dashboard

Este capítulo mostra o que é, para que serve o Dashboard do Aker Report Center.

O Dashboard do Aker Report Center foi projetado para oferecer maior transparência e facilidade no controle dos dados mais relevantes para sua empresa, auxiliando os administradores do Aker Report Center na gestão dos logs. Com uma grande variedade de Widgets o administrador pode montar seu Dashboard selecionando os Widgets que exibem os dados mais importantes de acordo com a necessidade de sua empresa.

O Dashboard possui três abas, que serão abordadas nas páginas a seguir:

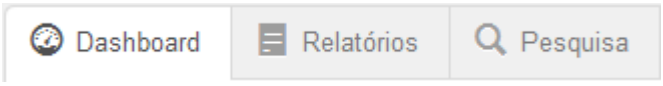


Figura 55 - Abas do Dashboard

3.1 *Aba Dashboard*

A aba Dashboard oferece transparência e facilidade no controle de dados para os gestores do Aker Report Center, permitindo que os mesmos possam configurar os Widgets de acordo com a necessidade de sua empresa, resumindo os dados mais importantes de uma entidade e seus respectivos ativos exibindo os dados nas mais diversas opções de gráficos disponíveis.

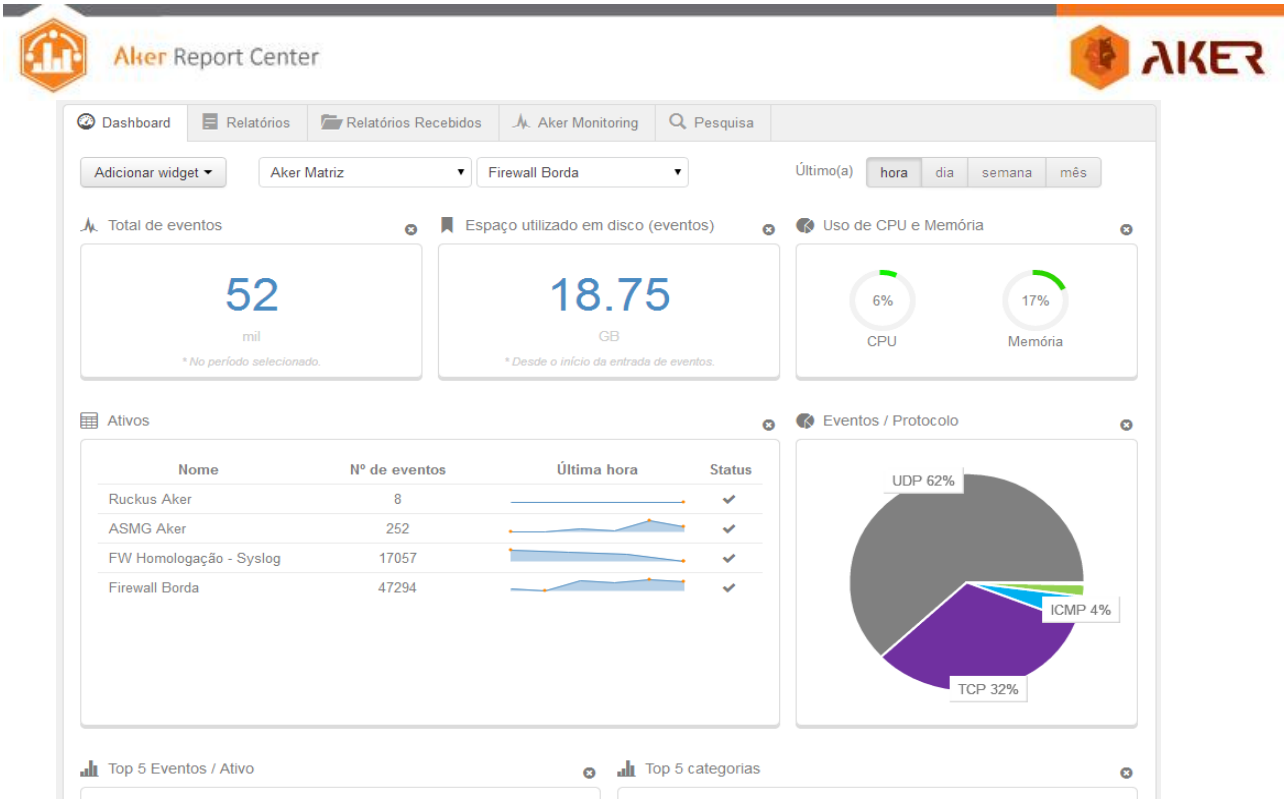


Figura 56 - Aba Dashboard

Na aba Dashboard existe um Widget que é atualizado em tempo real, exibindo os dados da máquina em tempo real facilitando a administração. “Este é: Uso de CPU e Memória”

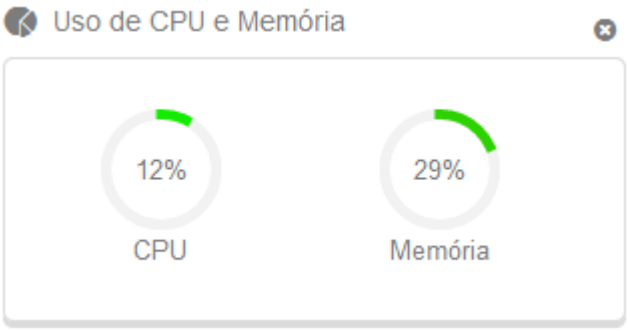


Figura 57 - Widgets atualizados em tempo real

O Widget “**Total de eventos**” exibe a quantidade de eventos de acordo com o período selecionado, as opções são: **Última hora, Último dia, Última semana e Último mês.**

Figura 58 – Widget “Total de eventos”

Figura 59 - Opções de período

E o Widget “***Espaço utilizado em disco (eventos)***” exibe o espaço utilizado em disco desde o início do recebimento de eventos do sistema.

Figura 60 - Widget "espaço utilizado em disco"

Os Widgets abordados acima “**Total de eventos, Espaço utilizado em disco, e Uso de CPU e Memória**” são as únicas exceções de configuração dos Widgets. Os demais Widgets são atualizados de forma consolidada a cada 5 minutos.

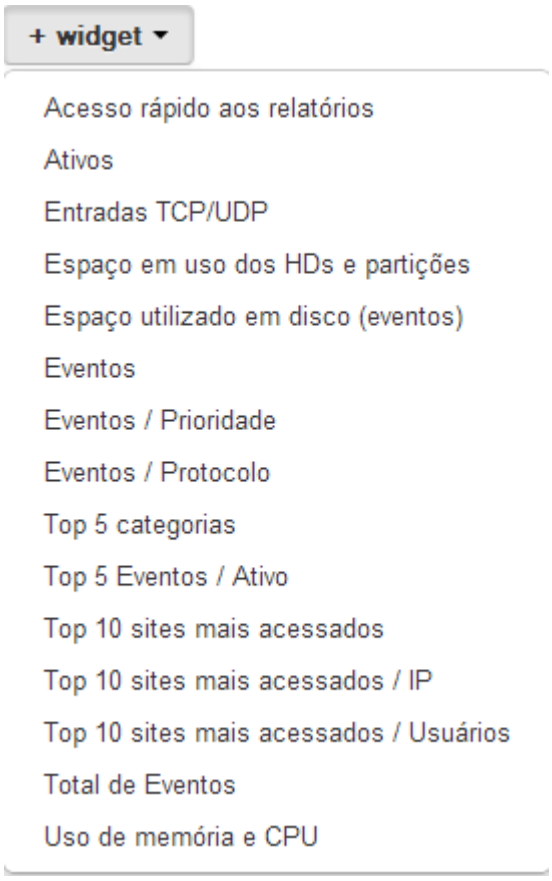


Figura 61 - Opções de Widget

3.2 *Aba Relatórios*

A aba "**Relatórios**" permite que o usuário selecione o relatório desejado entre os vários modelos disponíveis, facilitando e oferecendo rapidez na geração de relatórios. Entre os modelos estão: ***Sites mais acessados, IPs de origem, Sites mais bloqueados, Protocolo por IP, Categoria*** e outros, (***Veja o tópico Criar Relatório para saber mais sobre como criar Relatórios e Grupos de Relatórios***).

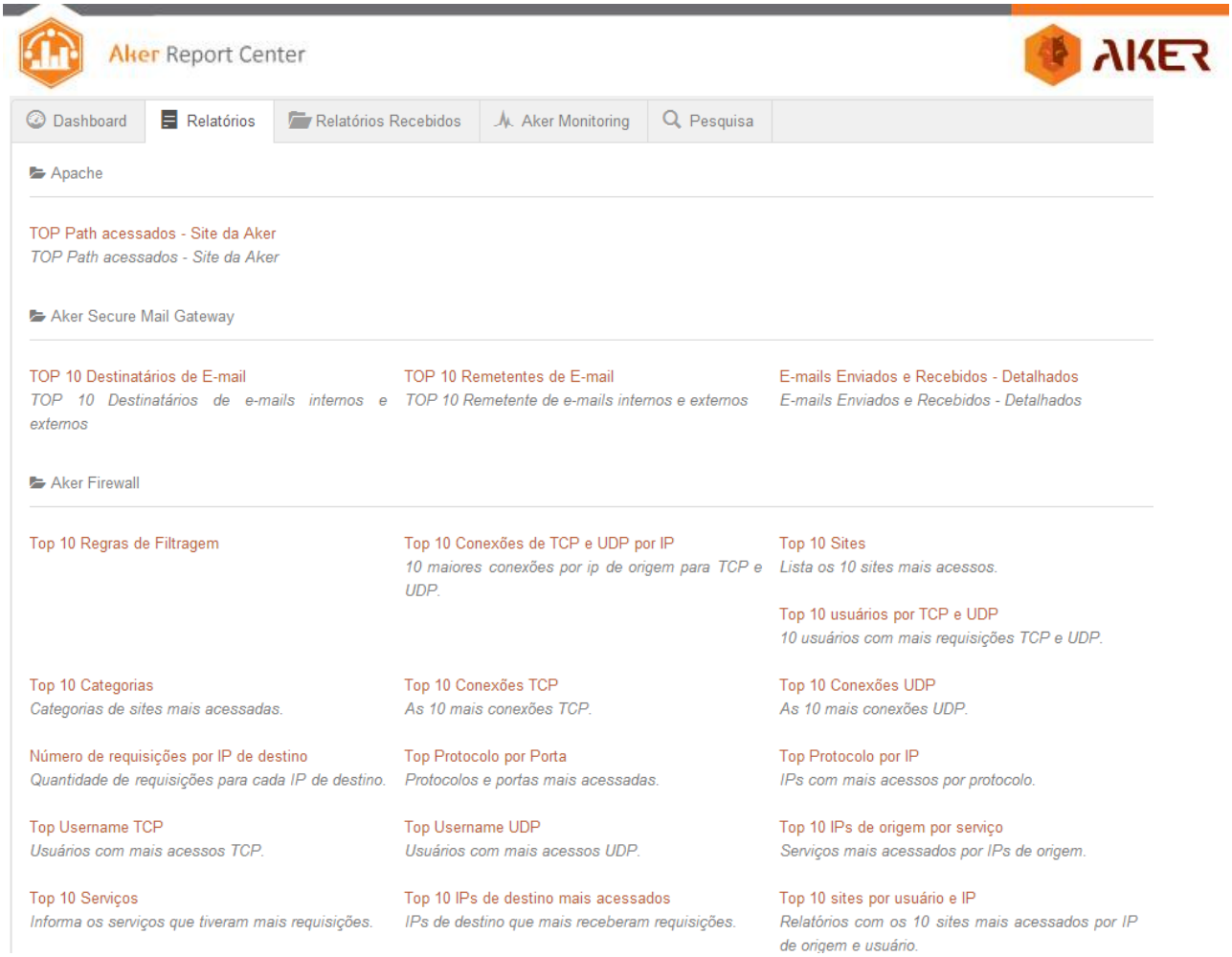

Aker Report Center
AKER
Dashboard
Relatórios
Relatórios Recebidos
Aker Monitoring
Pesquisa
Apache
TOP Path acessados - Site da Aker
TOP Path acessados - Site da Aker
Aker Secure Mail Gateway
TOP 10 Destinatários de E-mail
TOP 10 Destinatários de e-mails internos e externos
TOP 10 Remetentes de E-mail
TOP 10 Remetente de e-mails internos e externos
E-mails Enviados e Recebidos - Detalhados
E-mails Enviados e Recebidos - Detalhados
Aker Firewall
Top 10 Regras de Filtragem
Top 10 Conexões de TCP e UDP por IP
10 maiores conexões por ip de origem para TCP e UDP.
Top 10 Sites
Lista os 10 sites mais acessos.
Top 10 usuários por TCP e UDP
10 usuários com mais requisições TCP e UDP.
Top 10 Categorias
Categorias de sites mais acessadas.
Top 10 Conexões TCP
As 10 mais conexões TCP.
Top 10 Conexões UDP
As 10 mais conexões UDP.
Número de requisições por IP de destino
Quantidade de requisições para cada IP de destino.
Top Protocolo por Porta
Protocolos e portas mais acessadas.
Top Protocolo por IP
IPs com mais acessos por protocolo.
Top Username TCP
Usuários com mais acessos TCP.
Top Username UDP
Usuários com mais acessos UDP.
Top 10 IPs de origem por serviço
Serviços mais acessados por IPs de origem.
Top 10 Serviços
Informa os serviços que tiveram mais requisições.
Top 10 IPs de destino mais acessados
IPs de destino que mais receberam requisições.
Top 10 sites por usuário e IP
Relatórios com os 10 sites mais acessados por IP de origem e usuário.

Figura 62 - Aba Relatórios

O Aker Report Center oferece duas opções de ação para os usuários em questão aos relatórios, sendo elas, a visualização do relatório na própria página web, ou a exportação do relatório nos formatos HTML, TXT, ou PDF.

Todos os arquivos importados pelo Aker Report Center usam a codificação UTF-8.

A seguir exemplos das duas opções.

3.2.1 Visualizando um relatório

Ao selecionar o tipo de relatório desejado o usuário pode selecionar o período o qual será exibido no relatório, selecionando a Data de início, Data de fim, e tipo de ativo (*não é mandatório que as Data de início e Data de fim sejam definidas sendo possível definir apenas uma delas, e os filtros podem variar de acordo com tipo de relatório, estes filtros são definidos na criação do relatório*).

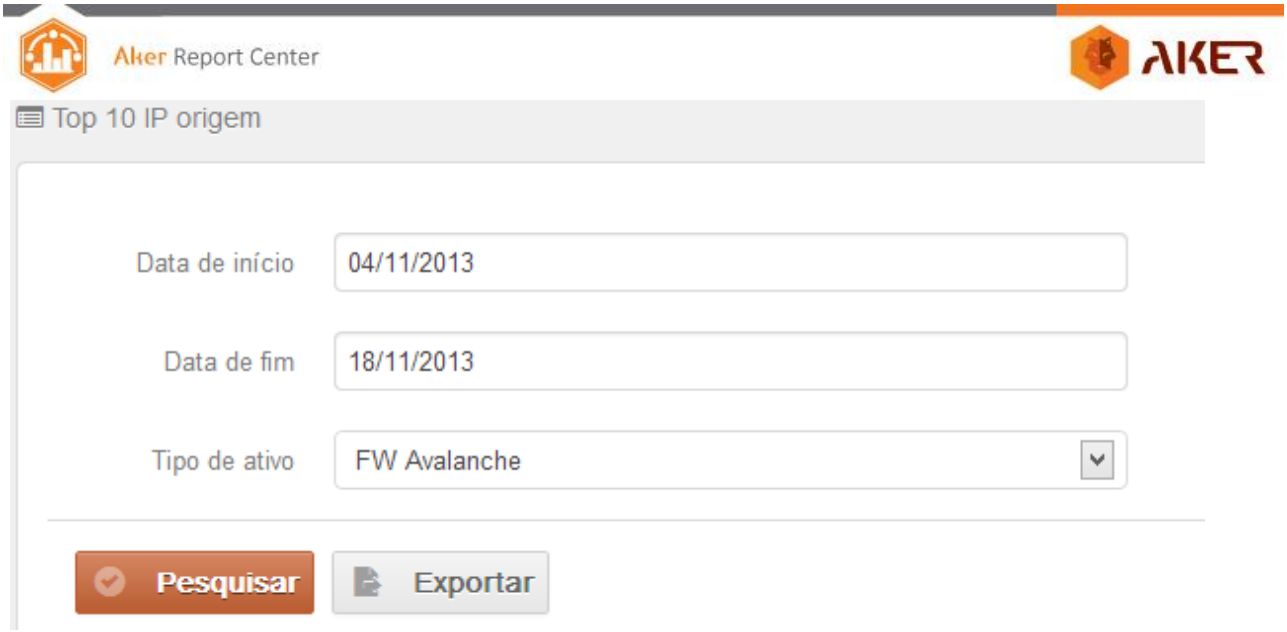


Figura 63 - Visualização de Relatórios

Data de início: Neste campo o usuário deve selecionar a data de início do relatório.

Ex: 04/11/2013 *(as informações contidas no relatórios serão a partir desta data)*

Data de fim: Neste campo o usuário deve selecionar a data de fim do relatório.

Ex: 18/11/2013 *(as informações contidas no relatórios serão até esta data)*

Tipo de ativo: Neste campo o usuário deve selecionar o ativo o qual terá suas informações exibidas no relatório.

Ao selecionar o período e o ativo de seu relatório, clique em "Pesquisar" para visualizar o relatório na página atual *(não é mandatório que as Data de início e Data de fim sejam definidas sendo possível definir apenas uma delas)*

Figura 64 - Botão pesquisar

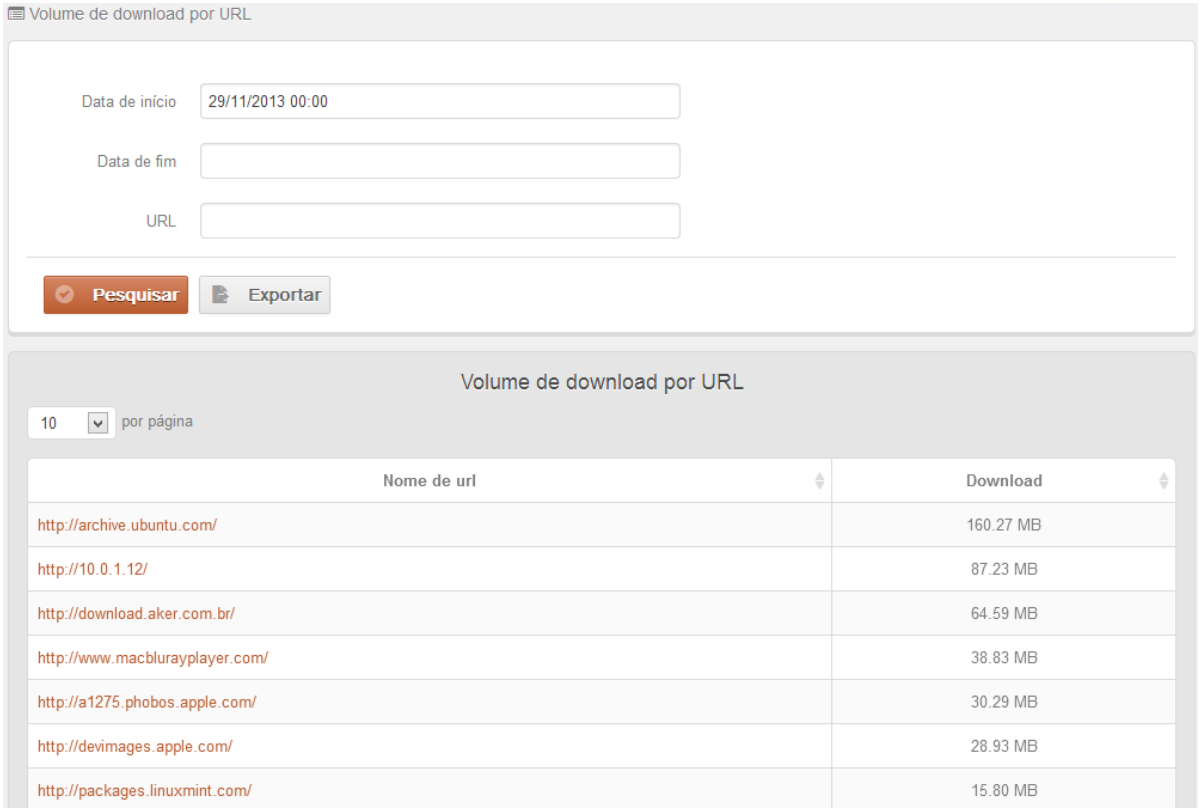


Figura 65 - Modelo de relatório (Volume de download por URL)

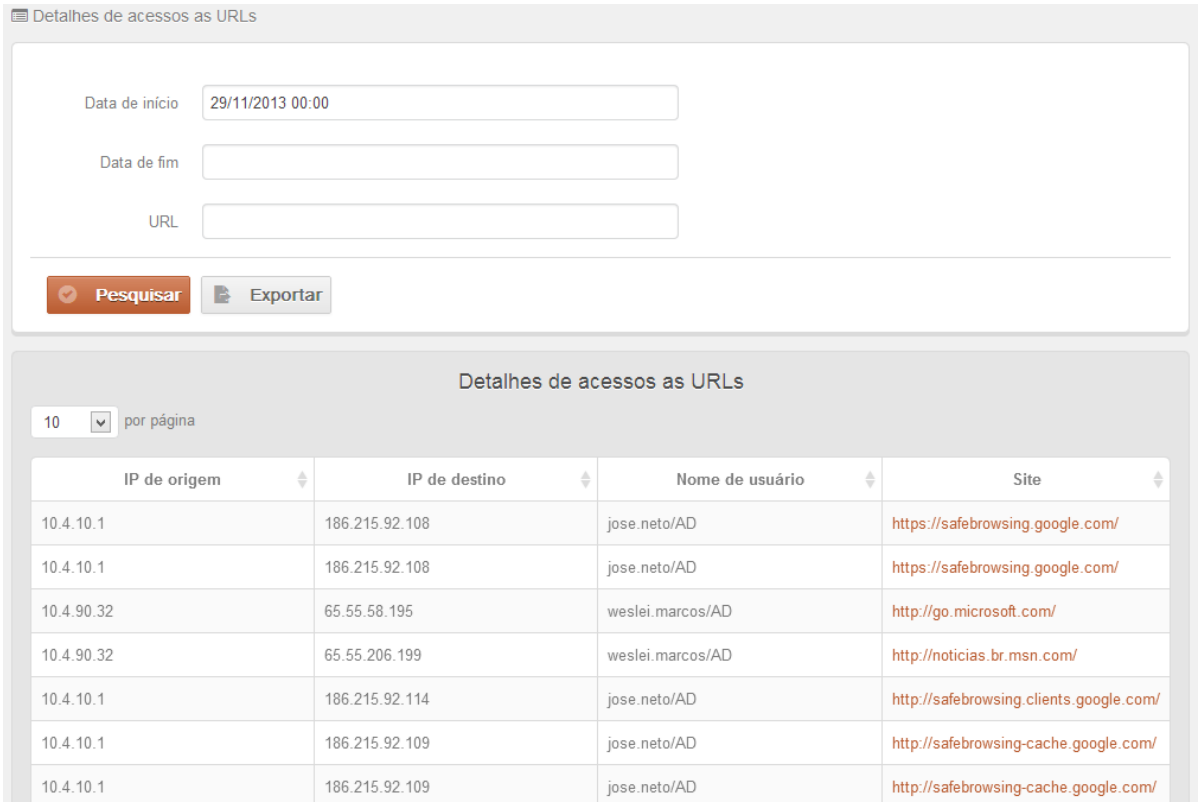


Figura 66 - Modelo de relatório (Detalhes de acessos as URLs)

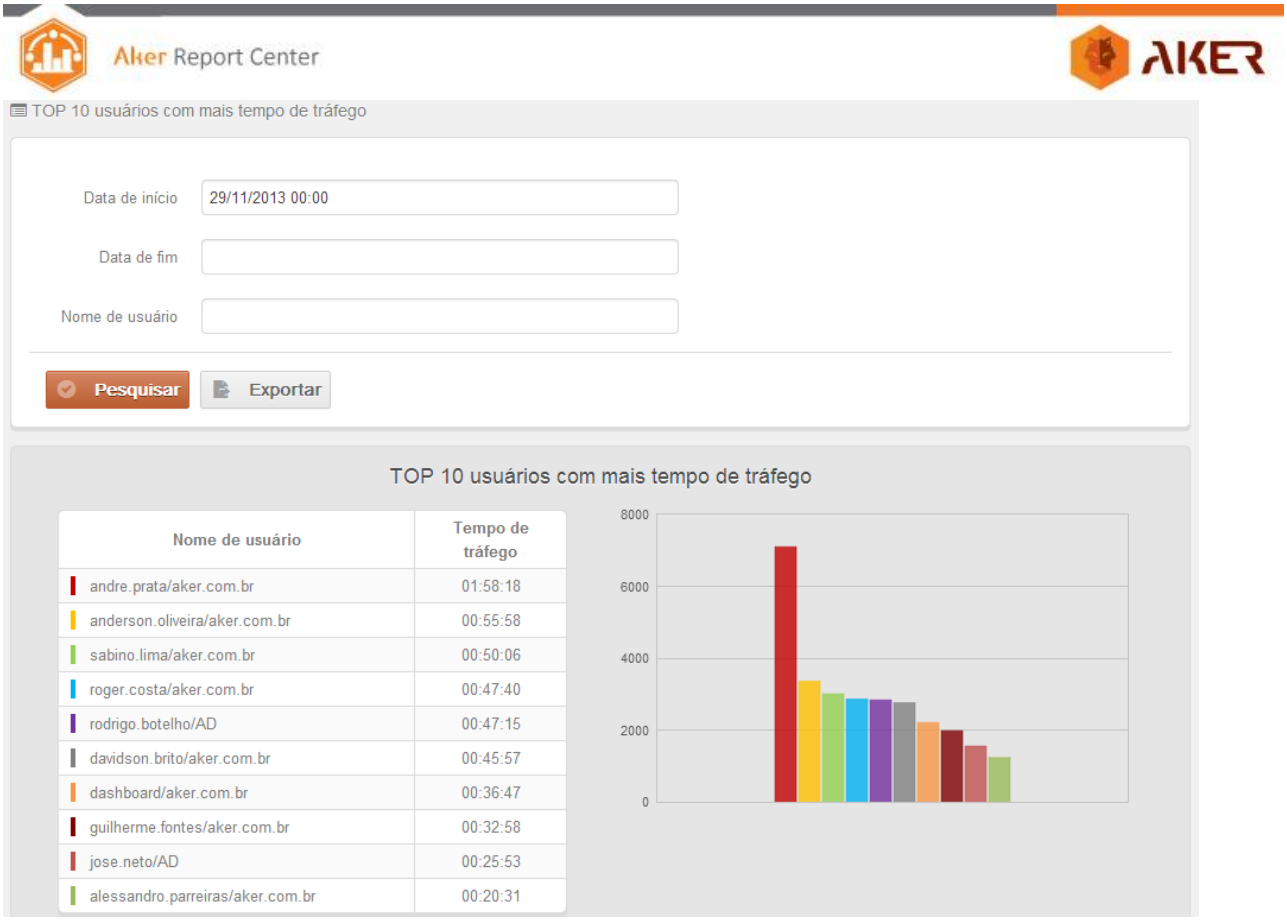


Figura 67 - Modelo de relatório (TOP 10 usuários com mais tempo de tráfego)

3.2.2 Exportando um relatório

Ao selecionar o tipo de relatório desejado o usuário pode selecionar o período o qual será exibido no relatório, selecionando a Data de início, Data de fim, e tipo de ativo (*não é mandatório que as Data de início e Data de fim sejam definidas sendo possível definir apenas uma delas, e os filtros podem variar de acordo com tipo de relatório, estes filtros são definidos na criação do relatório*).

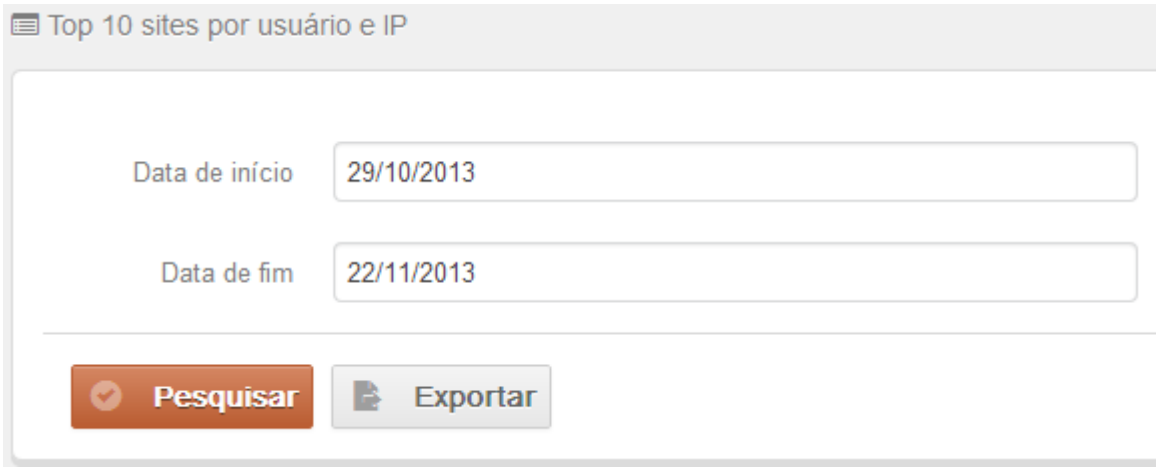


Figura 68 - Top 10 sites por usuário e IP

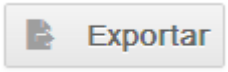


Figura 69 - Botão Exportar

Ao clicar no botão "***Exportar***" uma janela será exibida perguntando ao usuário qual o formato que o relatório será salvo. As opções disponíveis são: **HTML**, **TXT**, ou **PDF**.

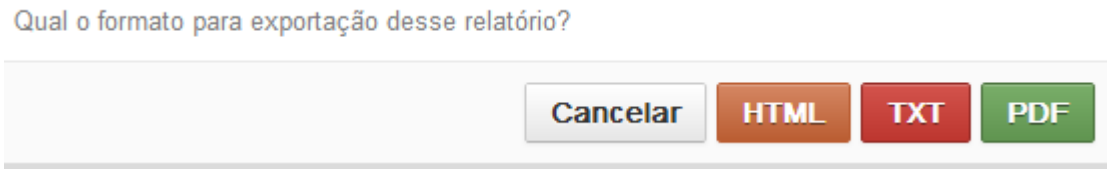


Figura 70 - Opções de formato de Relatório

Clique na opção desejada para que o download do relatório seja iniciado.

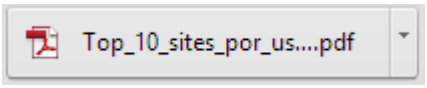
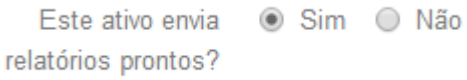


Figura 71 - Exportação de relatório (PDF)

3.3 *Aba Relatórios Recebidos*

Nesta aba o usuário pode ter acesso a todos os relatórios que foram recebido por outros ativos. Esta aba é dividida em duas partes que serão abordadas a seguir:

Para que um ativo tenha à permissão para enviar relatórios prontos para outros ativos, e necessário configura o mesmo, selecionando "***Sim***" para o opção "***Este ativo envia relatórios prontos***" na configuração do ativo para mais informação sobre cadastro de ativos veja o capitulo "**Cadastrando um novo ativo**"



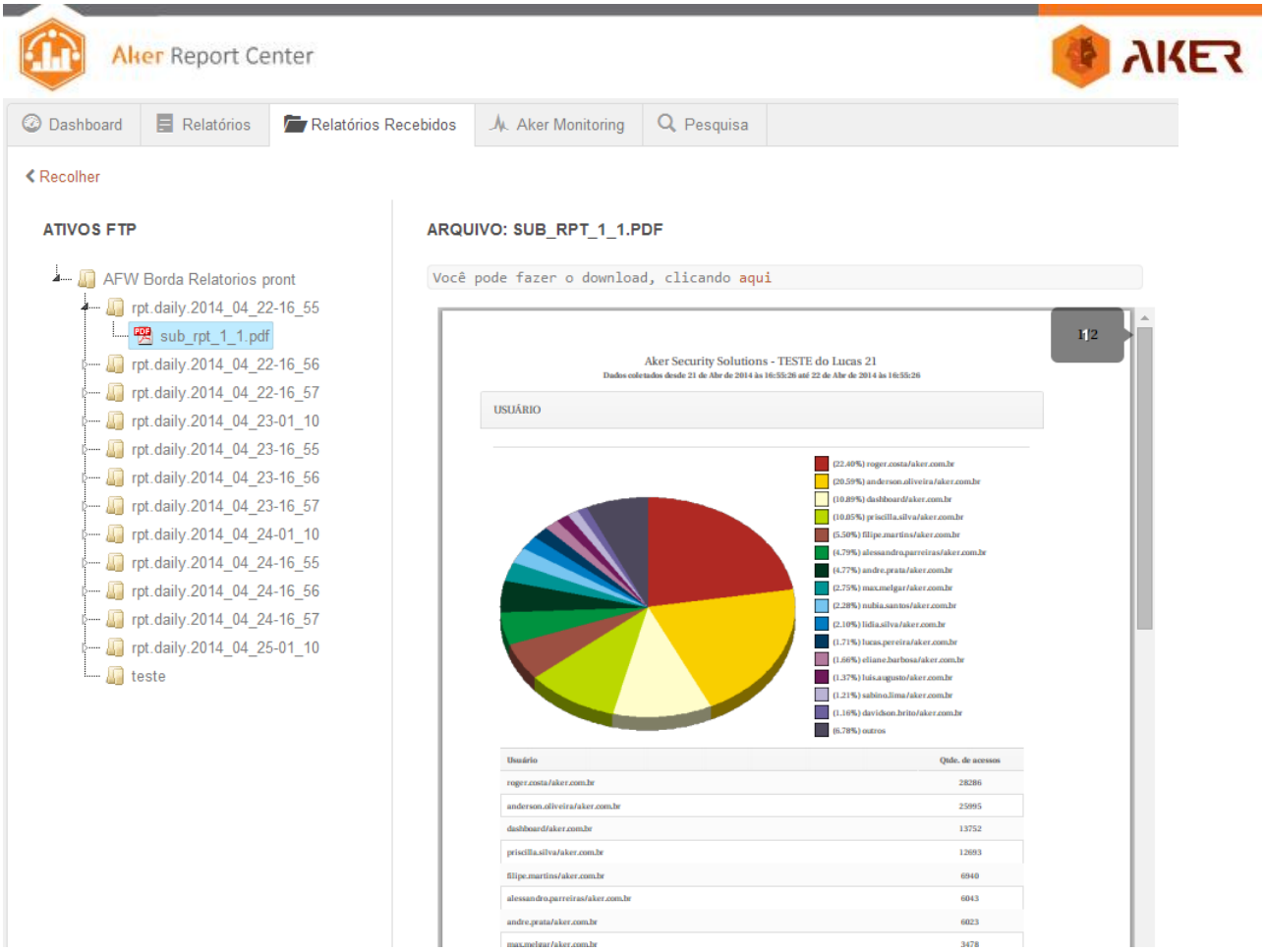


Figura 72 - Relatórios Recebidos

Ativos FTP

Nesta parte da aba de *Relatórios Recebidos* fica a lista de relatórios que foram recebidos por outros ativos.

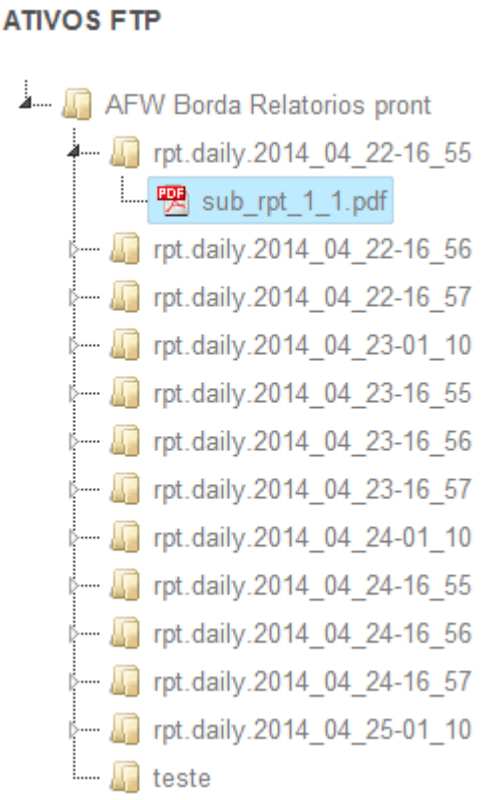


Figura 73 - Ativos FTP

Visualização de arquivos

Nesta parte da aba de *Relatórios Recebidos* o usuário pode visualizar o relatório selecionado na lista de *"Ativos FTP".*

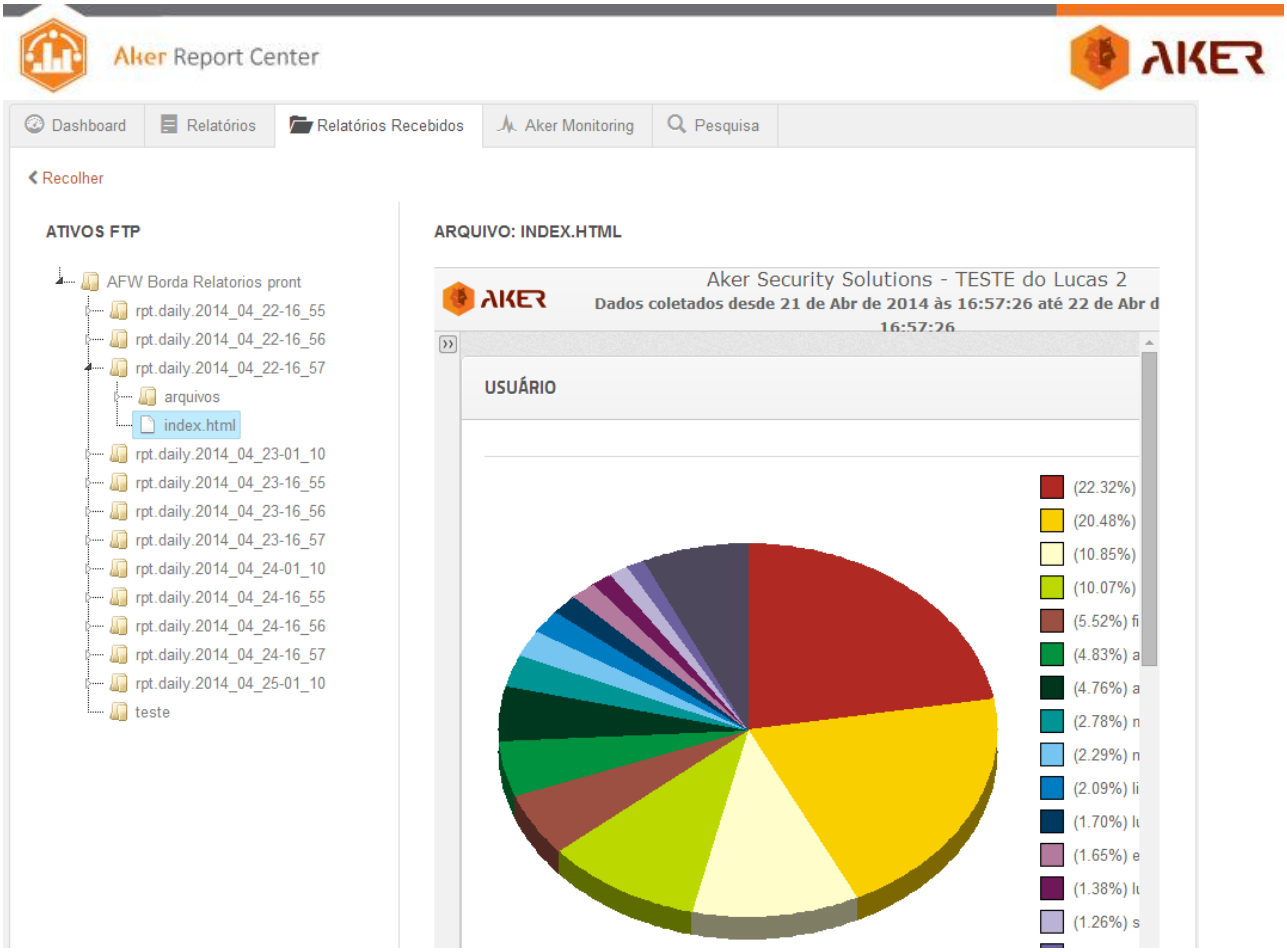


Figura 74 - Visualização de arquivos

3.4 *Aba Aker Monitoring*

A aba Aker Monitoring permite que o usuário faça um monitoramento especializados nos ativos, e um fácil e pratico gerenciamento integrado do seu ambiente tecnológico.

Por meio desta aba o usuário tem acesso em tempo real, ao sistema de monitoramento de ativos de rede, como: Servidores, Roteadores, Switches, Firewalls, e banco de dados SQL.

O Aker Monitoring Service envia todos os alertas para o centro de gerenciamento de redes da Aker, que aciona um analista técnico para solucionar (*além de enviar e-mails ou SMS ao detectar um problema*) os problemas detectados nos ativos de sua rede.

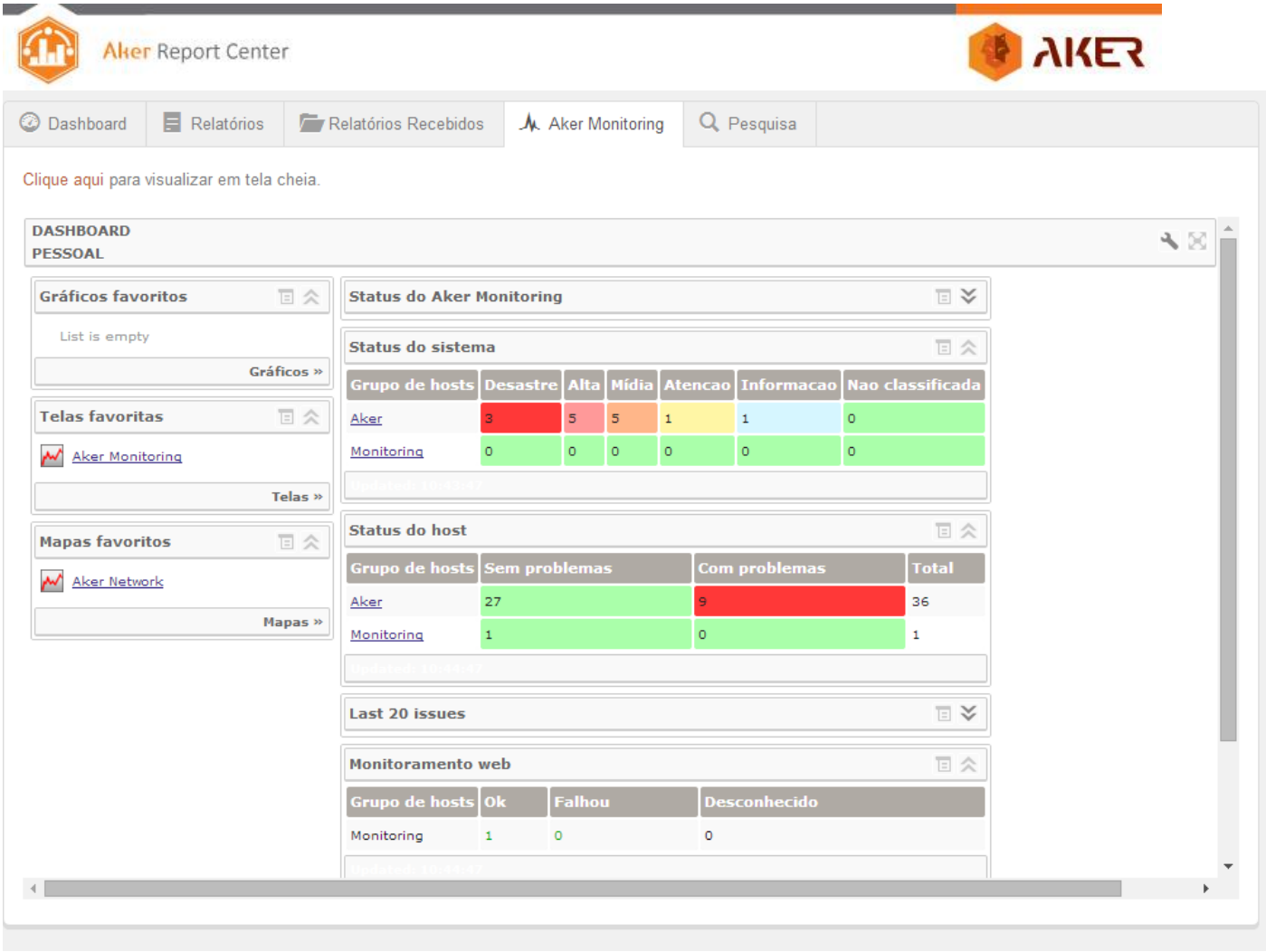


Figura 75 - Aker Monitoring

3.5 *Aba Pesquisa*

A aba pesquisa permite que o usuário faça pesquisa de valores (*Nomes de usuários, palavras, etc*,) diretamente nos logs armazenados. Para fazer a pesquisa é necessário que o usuário especifique:

- Ativo (*no exemplo abaixo: Firewall Borda*) no qual a pesquisa será feita,
- Não identificados - Definir se os logs os quais não formam reconhecidos pelo *Aker Report Center* serão exibidos na pesquisa abaixo, selecionando a opção Não identificados fará com que dados não reconhecidos sejam exibidos na pesquisa.
- Valor (*no exemplo abaixo: @gmail.com*) que será pesquisado,
- Período (no exemplo abaixo: De 01/04/2014 11:50 à 24/04/2014 06:30).

No campo ativo o usuário pode filtrar um ativo especifico ou efetuar a pesquisa em todos os ativos disponíveis, e não é mandatório selecionar as duas datas do período, podendo assim, selecionar uma ou outra.

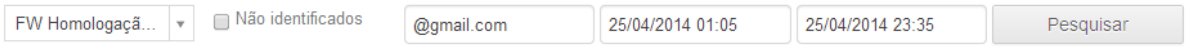


Figura 76 - Aba Pesquisa

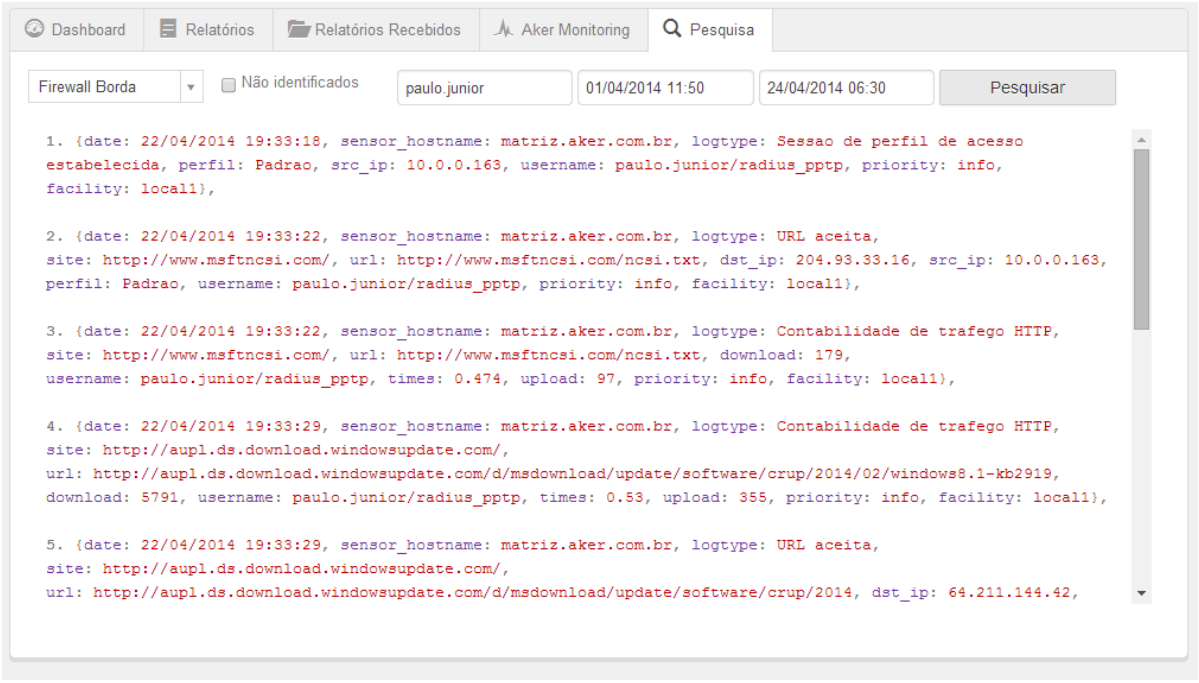

Dashboard
Relatórios
Relatórios Recebidos
Aker Monitoring
Pesquisa
Firewall Borda
Não identificados
paulo.junior
01/04/2014 11:50
24/04/2014 06:30
Pesquisar
1. {date: 22/04/2014 19:33:18, sensor_hostname: matriz.aker.com.br, logtype: Sessao de perfil de acesso estabelecida, perfil: Padrao, src_ip: 10.0.0.163, username: paulo.junior/radius_pptp, priority: info, facility: local1},
2. {date: 22/04/2014 19:33:22, sensor_hostname: matriz.aker.com.br, logtype: URL aceita, site: http://www.msftncsi.com/, url: http://www.msftncsi.com/ncsi.txt, dst_ip: 204.93.33.16, src_ip: 10.0.0.163, perfil: Padrao, username: paulo.junior/radius_pptp, priority: info, facility: local1},
3. {date: 22/04/2014 19:33:22, sensor_hostname: matriz.aker.com.br, logtype: Contabilidade de trafego HTTP, site: http://www.msftncsi.com/, url: http://www.msftncsi.com/ncsi.txt, download: 179, username: paulo.junior/radius_pptp, times: 0.474, upload: 97, priority: info, facility: local1},
4. {date: 22/04/2014 19:33:29, sensor_hostname: matriz.aker.com.br, logtype: Contabilidade de trafego HTTP, site: http://aupl.ds.download.windowsupdate.com/, url: http://aupl.ds.download.windowsupdate.com/d/msdownload/update/software/crup/2014/02/windows8.1-kb2919, download: 5791, username: paulo.junior/radius_pptp, times: 0.53, upload: 355, priority: info, facility: local1},
5. {date: 22/04/2014 19:33:29, sensor_hostname: matriz.aker.com.br, logtype: URL aceita, site: http://aupl.ds.download.windowsupdate.com/, url: http://aupl.ds.download.windowsupdate.com/d/msdownload/update/software/crup/2014, dst_ip: 64.211.144.42,

Figura 77 - Resultado da pesquisa

Relatórios

4 Relatórios

Este capítulo mostra como criar relatórios, fazer agendamentos e como criar grupos de relatórios.

O menu "***Relatórios***" permite que o usuário agende relatórios automáticos, crie seu próprio modelo de relatório, e crie grupos de relatórios.

Figura 78 - Opções do menu Relatórios

4.1 *Agendamento*

Na janela "***Agendamento***" o usuário pode visualizar os relatórios que já foram gerados no sistema, e configurar o agendamento automático de relatórios. A seguir mais informações sobre estas opções:

4.1.1 Relatórios gerados

A opção "***Relatórios gerados***" permite que o usuário visualize os relatórios que foram gerados no sistema do Aker Report Center.

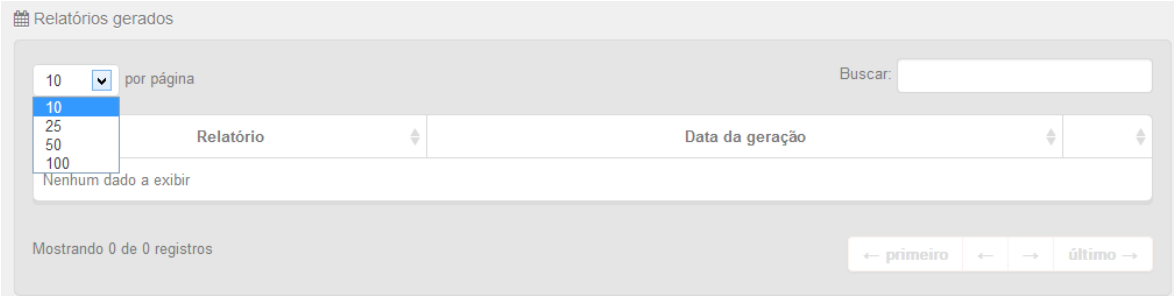


Figura 79 - Relatórios gerados

4.1.2 Agendar

Na janela "***Agendar***" é possível que o usuário edite, exclua, ou crie um novo agendamento.

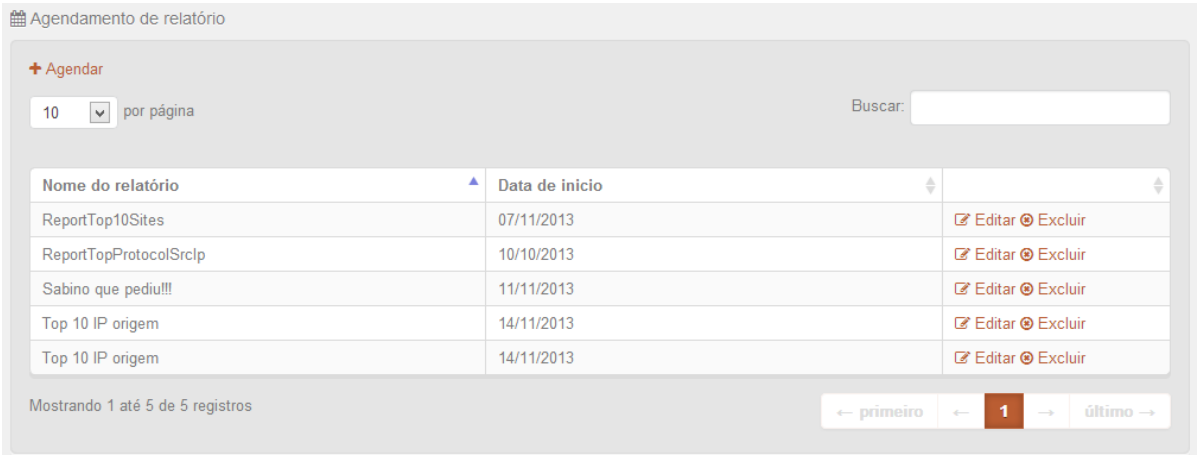


Figura 80 - Agendamento de relatório

4.1.3 Agendando um novo relatório

Para agendar um novo relatórios siga os passos a seguir:

- Clique em + Agendar, e então preencha os campos exibidos na imagem a seguir corretamente:

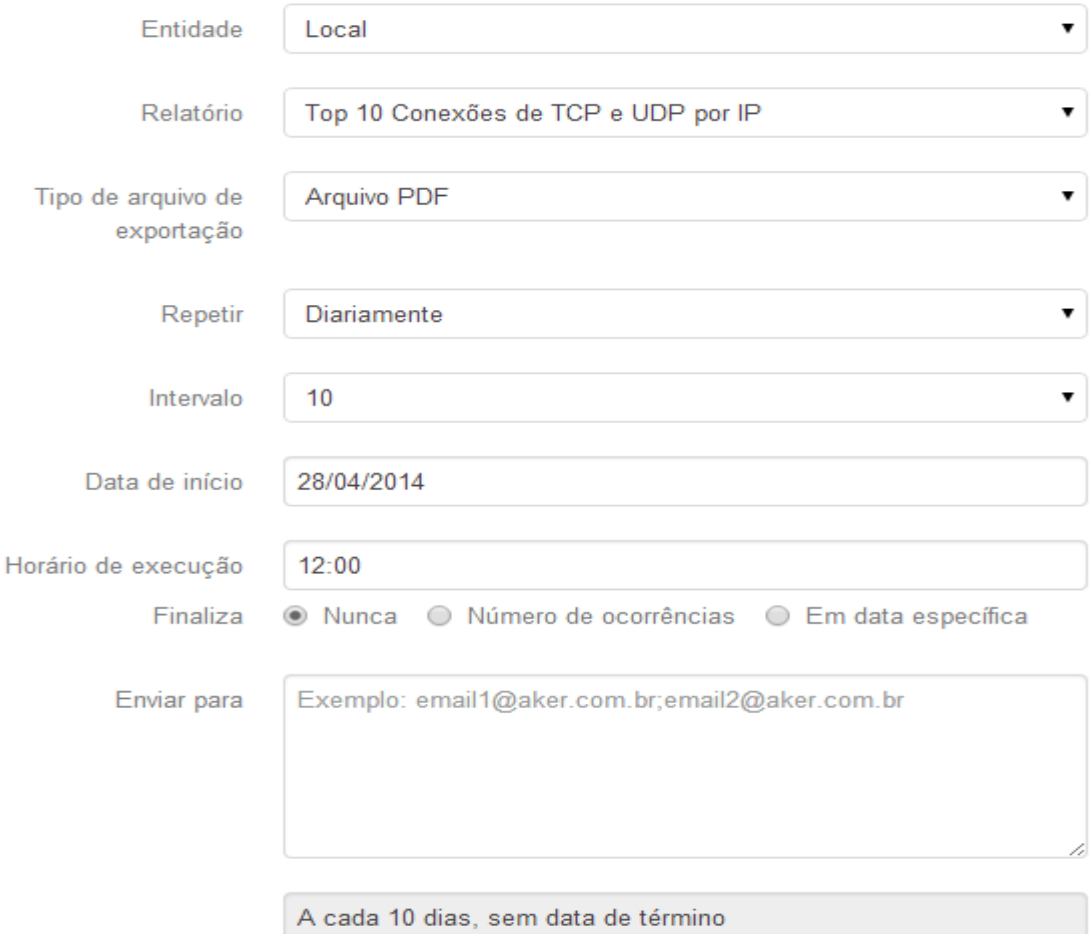


Figura 81 - Agendamento de relatórios

Entidade: Neste campo o usuário deve selecionar a entidade da qual o relatório será gerado;

Relatório: Neste campo o usuário deve selecionar qual o relatório que será feito automaticamente.

Tipo de arquivo de exportação: Neste campo o usuário deve selecionar qual será o tipo de arquivo de exportação do relatório, as opções disponíveis são: Formato de texto, Página HTML, ou Arquivo PDF.

Repetir: Neste campo o usuário deve selecionar qual será a frequência que o agendamento será feito, as opções disponíveis são: Diariamente, Semanalmente e mensalmente.

Intervalo: Neste campo o usuário deve definir o intervalo de tempo que o relatório será feito;

Exemplo:

Repetir diariamente/ Intervalo 10 = Este relatório será feito a cada 10 dias;

Repetir mensalmente / intervalo 3 = A Este relatório será feito a cada 3 meses;

Data de início: Neste campo o usuário deve selecionar qual será a data de início do relatório.

Horário de execução:

Finalizar: Neste campo o usuário deve selecionar quando o relatório será finalizado, as opções são:

Nunca: Ao selecionar esta opção data o relatório não terá data de término;

Número de ocorrências – Ao selecionar esta opção deve-se informar o número de ocorrências para finalizar o relatório.

Em data específica – Ao selecionar esta opção deve se informar a "***data de fim***" do relatório.

Enviar para e-mail: Neste campo o usuário deve selecionar qual será o e-mail que receberá o relatório.

Parâmetro de pesquisa: Neste campo o usuário pode selecionar parâmetro especifico para ser exibido no relatório.

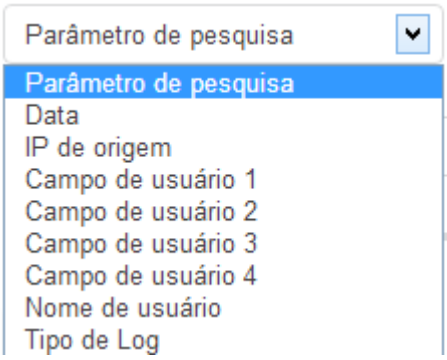


Figura 82 - Opções de parâmetros de pesquisa

Operador: Neste campo o usuário deve selecionar o operador que será usado na filtragem, segue as opções disponíveis:

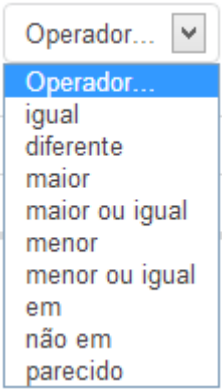


Figura 83 – Operador

4.2 *Relatórios gerados*

Esta janela exibe todos os Relatórios que foram gerados, e permite que o usuário faça o download ou delete o Relatório desejado.

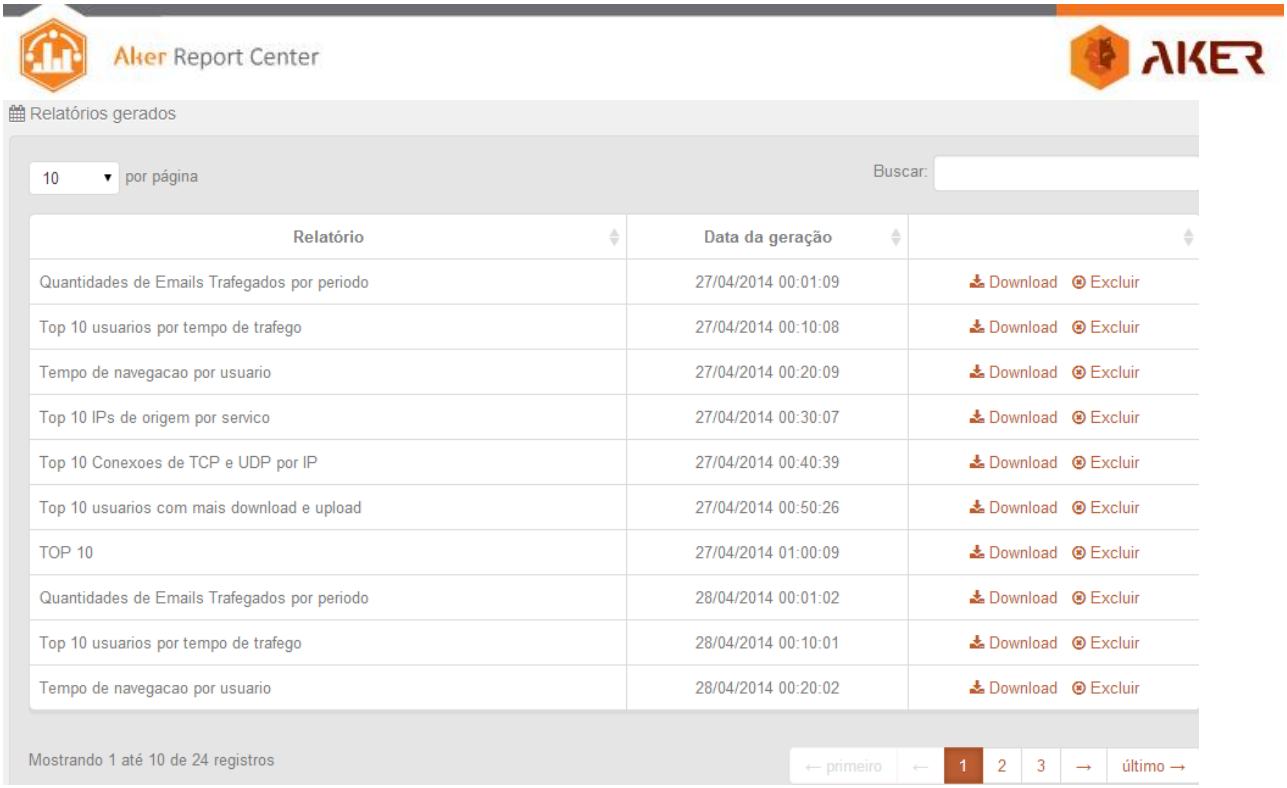

Aker Report Center
AKER
Relatórios gerados
10 por página
Buscar:
Relatório
Data da geração
Quantidades de Emails Trafegados por periodo 27/04/2014 00:01:09
Top 10 usuarios por tempo de trafego 27/04/2014 00:10:08
Tempo de navegacao por usuario 27/04/2014 00:20:09
Top 10 IPs de origem por servico 27/04/2014 00:30:07
Top 10 Conexoes de TCP e UDP por IP 27/04/2014 00:40:39
Top 10 usuarios com mais download e upload 27/04/2014 00:50:26
TOP 10 27/04/2014 01:00:09
Quantidades de Emails Trafegados por periodo 28/04/2014 00:01:02
Top 10 usuarios por tempo de trafego 28/04/2014 00:10:01
Tempo de navegacao por usuario 28/04/2014 00:20:02
Download Excluir
Mostrando 1 até 10 de 24 registros
primeiro 1 2 3 último

Figura 84 - Relatórios gerados

4.3 *Criar Relatório*

Na janela "***Criar Relatório***" é possível que o usuário visualize, edite, exclua os tipos de relatórios existentes no sistema. E ainda permite a criação de novos tipos de relatórios.

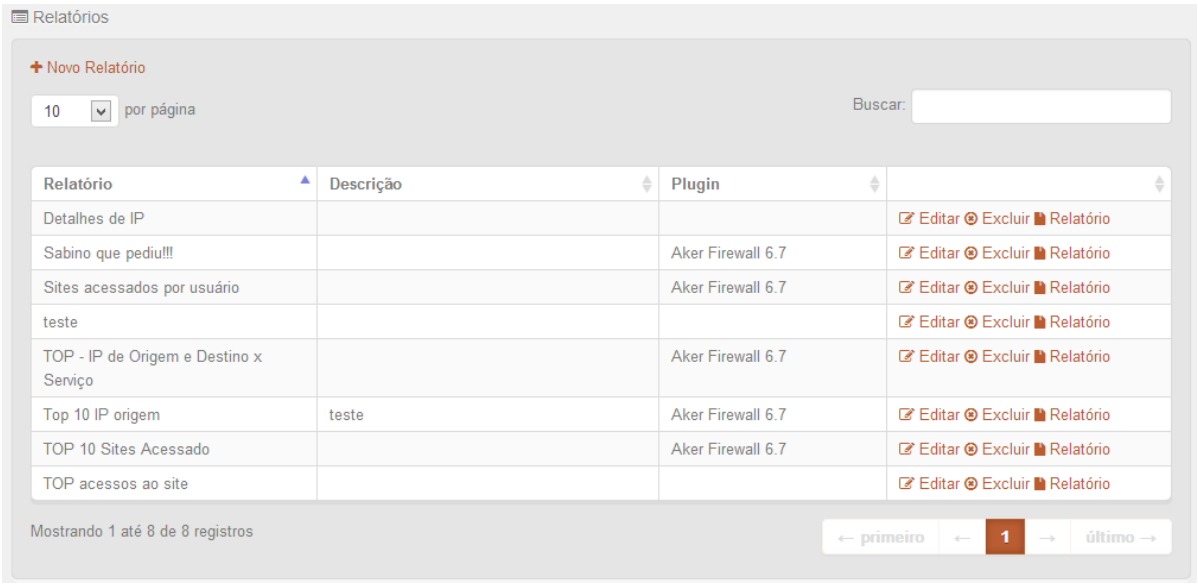
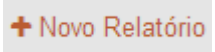


Figura 85 - Relatórios

4.3.1 Criando um novo tipo de relatório

Para criar um novo tipo de relatório siga os passos a seguir:

- Clique em 

, e preencha os campos das abas abaixo corretamente:

4.3.2 Aba Relatório

Nesta aba o usuário deve definir as informações básicas do novo relatório como: qual será o grupo, nome e tipo do relatório.

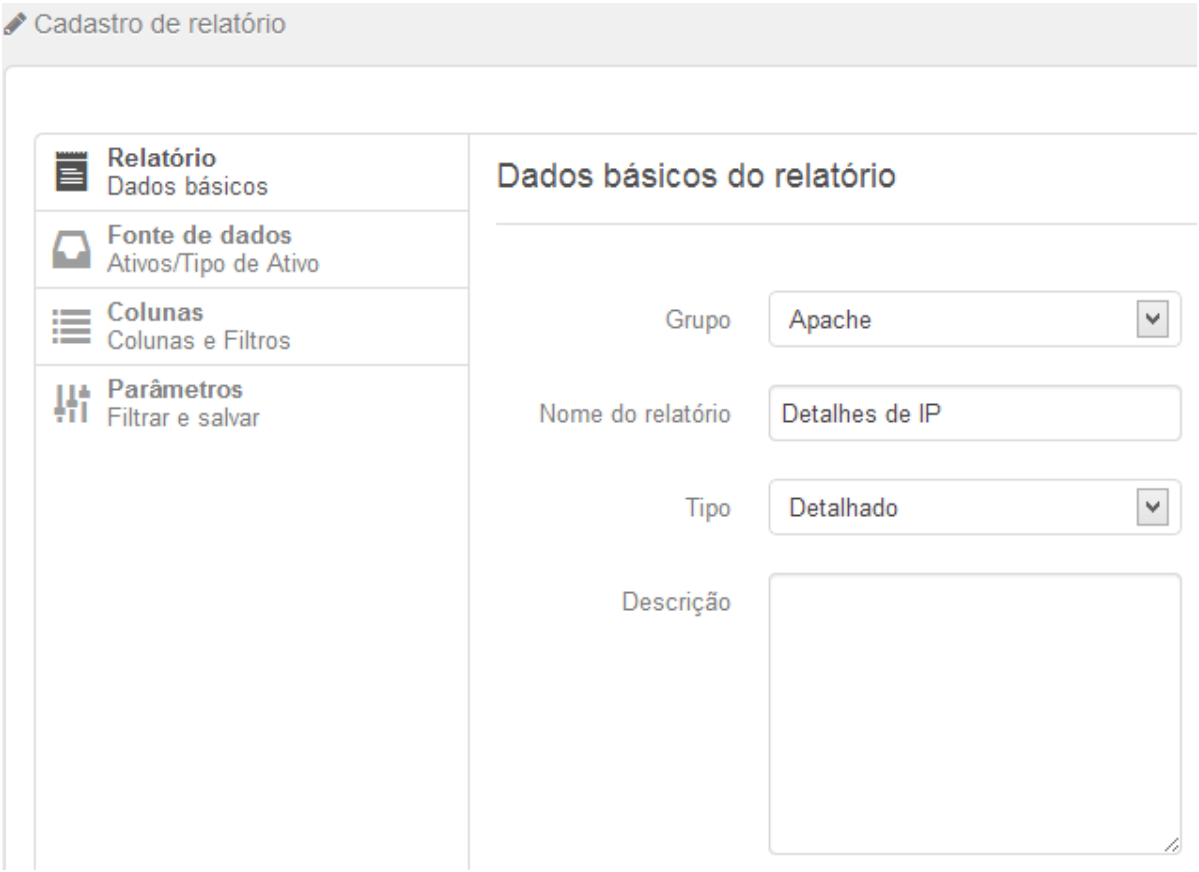


Figura 86 - Aba Relatório

Grupo: Neste campo o usuário deve selecionar qual o grupo que o relatório pertencerá. (*Mais informações sobre grupos de relatório no próximo tópico – 6.2 Grupos de relatórios)*

Nome do relatório: Neste campo o usuário deve definir qual será o nome do relatório.

Tipo: Neste campo o usuário deve selecionar qual será o tipo do relatório, podendo ser: Detalhado ou consolidado.

Descrição: Neste campo o usuário pode inserir descrições sobre o relatório que está sendo criado.

Ao preencher os dados acima corretamente, clique em **Próximo**.

4.3.3 Aba Fonte de dados

Nesta aba o usuário o usuário deve selecionar qual o ativo ou tipos de ativos que serão carregados no relatório.

Figura 87 - Aba Fonte de dados

Ao selecionar os ativos desejados, cliquem em **Próximo**.

4.3.4 Aba Colunas

Nesta aba o usuário o usuário deve selecionar as informações que serão ou não exibidas nas colunas do relatório.

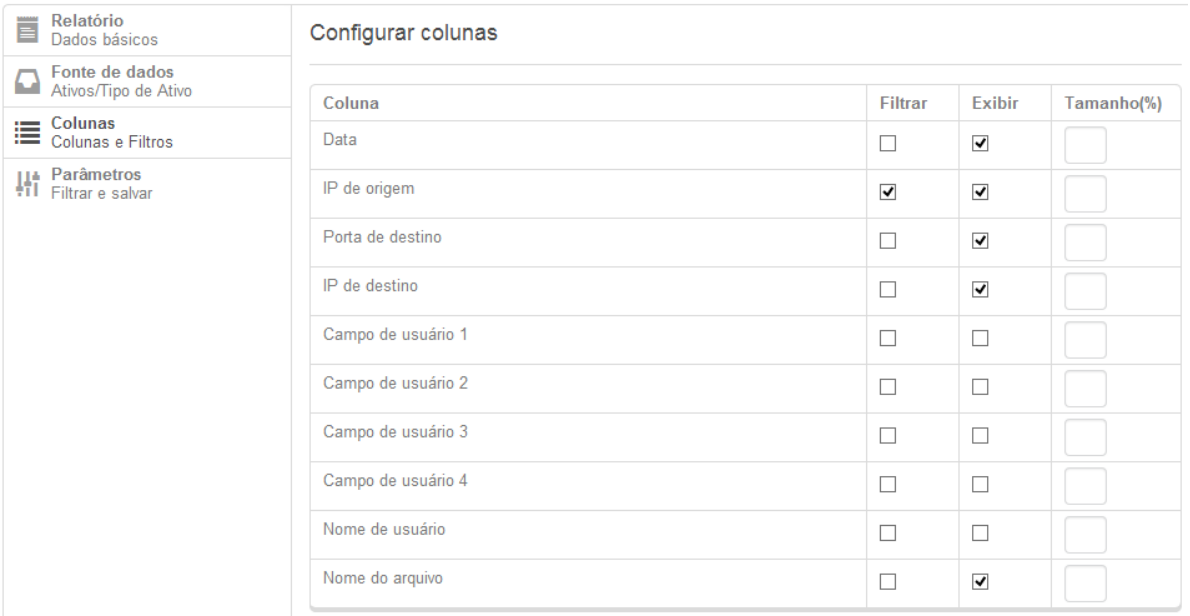


Figura 88 - Aba Colunas

Filtrar: Nesta coluna o usuário deve selecionar quais as informações que serão filtradas no relatório, ou seja, filtros que serão exibidos no formulário de pesquisa do relatório em criação.

Exibir: Nesta coluna o usuário deve selecionar quais as informações que serão exibidas no relatório.

Tamanho: Nesta coluna o usuário deve definir qual a porcentagem que determinada informação irá ocupar no relatório.

A ordem das colunas pode ser alterada usando drag and drop.

4.3.5 Aba Parâmetros

Nesta aba o usuário o usuário deve selecionar quais os parâmetros serão filtrados para exibir em seu relatório.

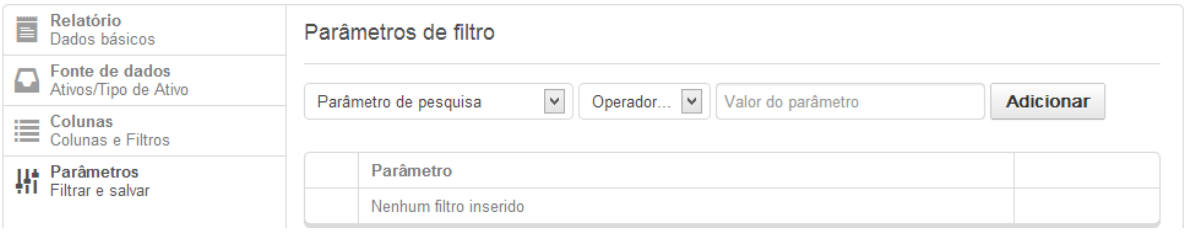


Figura 89 - Aba Parâmetros de filtro

Parâmetro de pesquisa: Neste campo o usuário pode selecionar um parâmetro especifico para ser exibido no relatório.

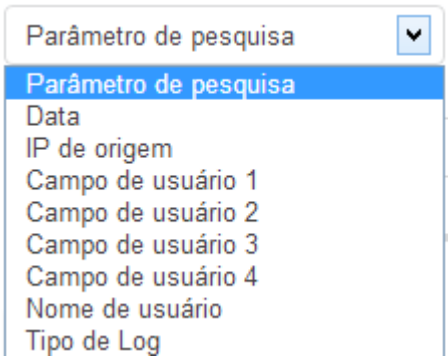


Figura 90 - Opções de parâmetros de pesquisa

Operador: Neste campo o usuário deve selecionar o operador que será usado na filtragem, segue as opções disponíveis:

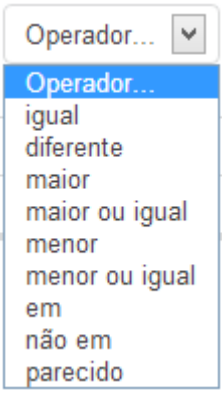


Figura 91 - Operador

Clique no botão "*Adicionar*" para concluir a inserção do parâmetro.

Ao preencher e configurar as abas acima corretamente, clique em Salvar.

4.4 Grupos de relatórios

Esta opção permite que o usuário visualize ou crie grupos de relatórios, organizando seus relatórios em seus respectivos grupos.

Figura 92 - Grupos de relatórios

4.4.1 Criando um novo grupo de Relatório

Para criar um novo grupo de Relatórios siga os passos a seguir:

- Clique em Novo Grupo de Relatório:

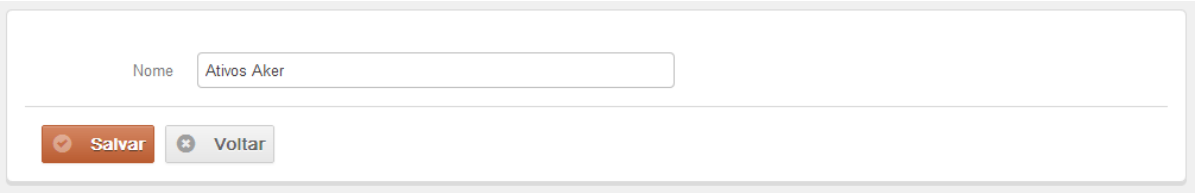


Figura 93 - Criando novo grupo de relatório

- No campo "*Nome*" insira o nome desejado para o seu grupo de relatórios
- Clique em Salvar.

4.5 Logs do sistema

Na janela "***Logs do sistema***" é possível que o usuário visualize as ações que foram feitas no sistema do Aker Report Center.

Logs do sistema
10
por página
Buscar:
Data
Tipo
Mensagem
24/01/2014 11:55:07 Info O relatório 6 foi gerado.
24/01/2014 11:55:07 Info Apagando item da fila de id: '10'.
24/01/2014 11:47:47 Info Foi solicitada a geração do relatório 6.
24/01/2014 11:47:47 Info Iniciando geração do relatório: 6
24/01/2014 11:47:23 Info O usuário admin criou/alterou um relatório.
24/01/2014 11:45:37 Info O relatório 1 foi gerado.
24/01/2014 11:45:37 Info Apagando item da fila de id: '9'.
24/01/2014 11:44:18 Info Iniciando geração do relatório: 1
24/01/2014 11:44:17 Info Foi solicitada a geração do relatório 1.
24/01/2014 11:43:40 Info O usuário admin excluiu o relatório de id 100000.
Mostrando 1 até 10 de 82 registros
← primeiro
1
2
3
4
5
→
último →

Figura 94 - Logs do sistema

Configurações

5 Configurações

Este capítulo mostra como configurar as variáveis dos sistema do Aker Report Center.

O menu "***Configurações***" permite que o usuário defina as configurações das entidades, ativos cadastrados, opções de backup, controle de acesso e logs, personalização do Aker Report Center, e as opções de segurança.

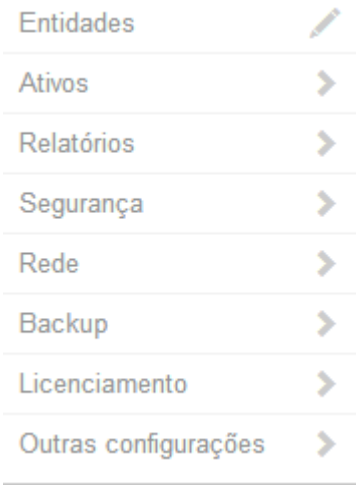
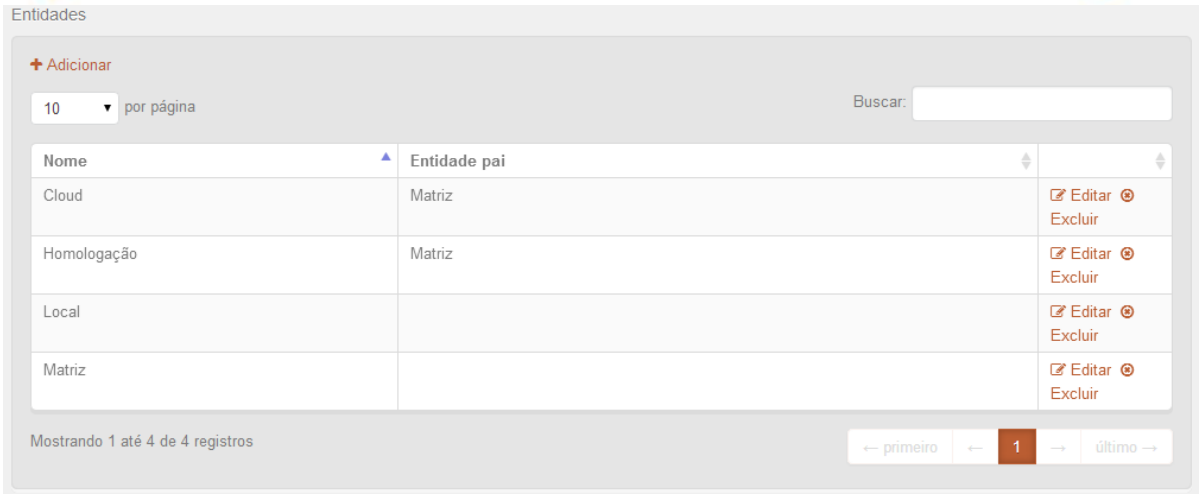


Figura 95 - Opções do menu Configurações

5.1 *Entidades*

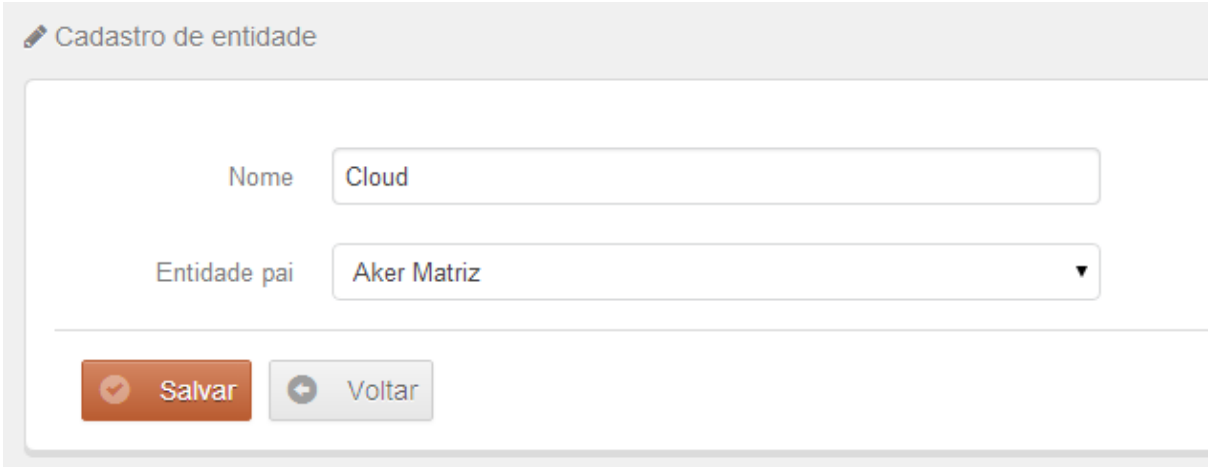
Neste submenu o usuário pode criar, editar, ou deletar "Entidades" que serão usadas nos filtros para geração de relatórios. Estas "*Entidades*" podem ser setores dentro da empresa, matrizes, filiais, Firewalls, ou qualquer outro local que possuam ativos designados ao mesmo.



Para inserir uma nova entidade clique em

.

A janela a seguir será exibida:



Nome: Neste campo o usuário deve inserir o nome de sua nova entidade;

Ex: Office Brasília, Homologação, Firewall de borda, Firewall de produção, Cloud, Matriz, Filial Goiânia e etc.,

Entidade pai: Neste campo o usuário pode selecionar uma entidade pai para a nova entidade. Esta entidade receberá os dados da entidade em criação, possibilitado o gerenciamento centralizados de vários Report Centers;

5.2 *Ativos*

O submenu "***Ativos***" permite que o usuário crie, edite ou delete "*Ativos*" no Aker Report Center. O menu "*Ativos*" possui três janelas de configuração que serão abordadas nas páginas a seguir:

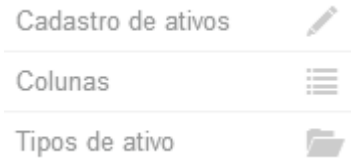


Figura 96 - opções do submenu Ativos

5.2.1 Cadastro de Ativos

A janela "*Cadastro de Ativos*" permite que o usuário visualize os ativos cadastrados no sistema, edite, delete ou adicione novos ativos. A seguir mais detalhes sobre como inserir um novo ativo no sistema do **Aker Report Center**:

Figura 97 - Cadastro de ativos

5.2.2 Cadastrando um novo Ativo

Para cadastrar um novo ativo siga os passos a seguir:

- Clique em para que a janela de cadastro a seguir seja exibida:

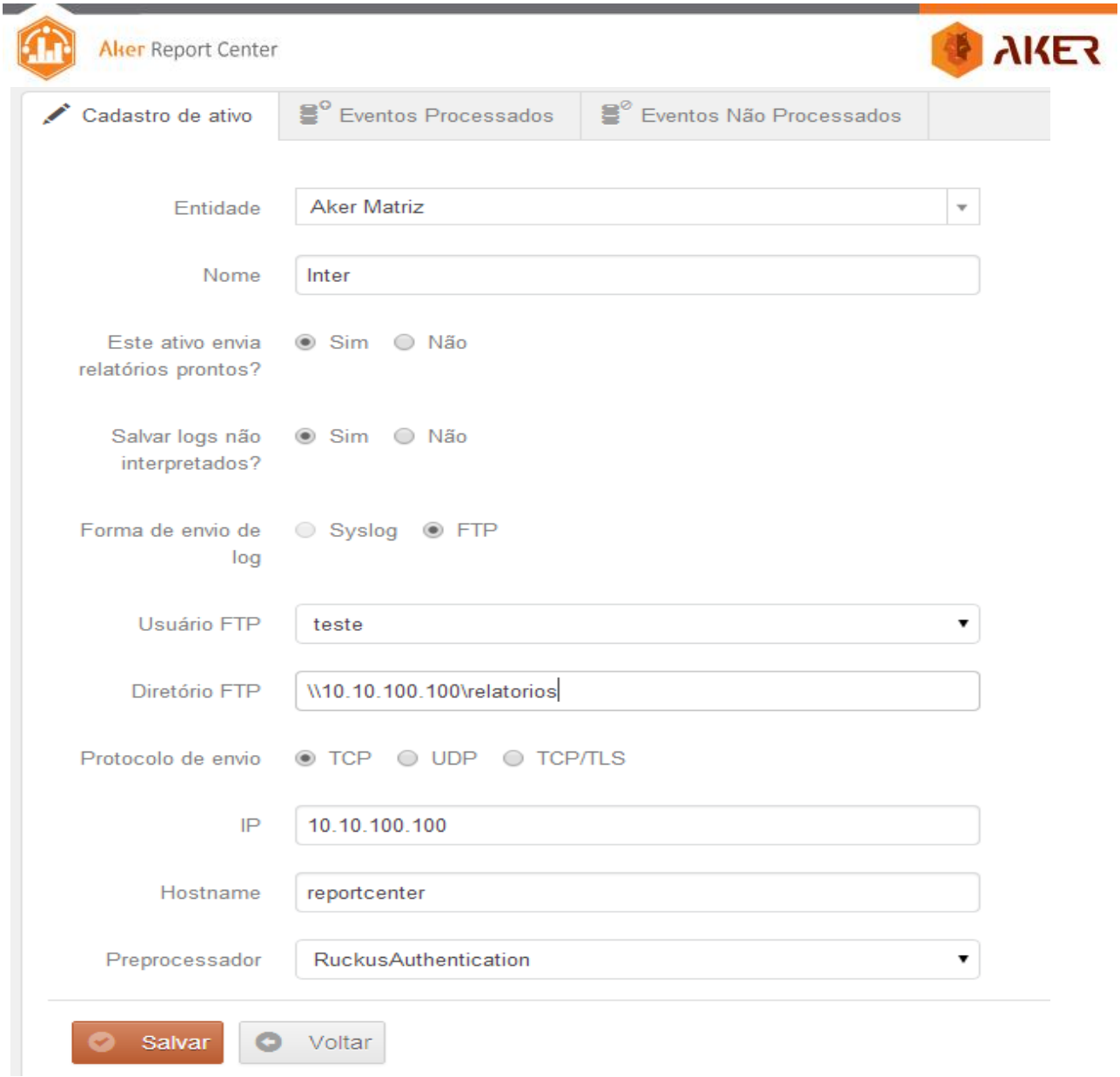


Figura 98 - Aba Cadastro de ativo

- Preencha os campos de aba "*Cadastro de ativo*" corretamente com a informação do ativo desejado, e clique em "***Salvar***". A seguir detalhes dos campos da janela acima:

5.2.3 Aba Cadastro de ativo

Nesta aba o usuário deve inserir as informações referentes ao ativo que será cadastrado corretamente:

Entidade: Neste campo o usuário deve selecionar uma entidade a qual este novo ativo irá pertencer (para mais informações sobre Entidade veja o capitulo "Entidades")

Nome: Neste campo deve ser inserido o nome do novo "*Ativo*" que será cadastrado.

Este ativo envia relatórios prontos: Neste campo deve-se definir se este ativo terá permissão para enviar relatórios prontos para outros ativos, às opções disponíveis são: ***Sim e Não***.

Ao selecionar "*Sim*" os logs e arquivos gerados por esse ativo que forem enviados poderão ser acessados na aba de relatórios recebidos (Dashboard). Quando essa opção está ativa, somente poderão ser enviados logs via FTP.

Salvar logs não interpretados: Neste campo deve-se definir se este ativo terá permissão para Salvar logs que não foram interpretados, ou seja, logs os quais não formam reconhecidos pelo *Aker Report Center*, as opções disponíveis são: **Sim e Não**.

Tipo de ativo: Neste campo deve-se selecionar qual o tipo do ativo que está sendo criado.

Forma de envio de log: Nesta opção o usuário deve selecionar qual será o método de envio de log. As opções disponíveis são **Syslog e FTP (**para mais informações sobre como cadastrar **usuários FTP e configuração Syslog,** veja o capitulo **7.17 Segurança****)**

O envio de logs via FTP é apenas possível para arquivos '**.TXT'**, ou seja, o sistema somente enviará arquivos (**.TXT)**, arquivos em formatos diferentes não serão considerados pelo sistema, sendo assim, não gerarão eventos.

Ao selecionar a opção de envio FTP é necessário informar o nome do usuário FTP e o ***caminho do diretório FTP*** *(no caminho do diretório não pode conter caracteres especiais, caso haja o sistema irá retira-los).*

Envio FTP

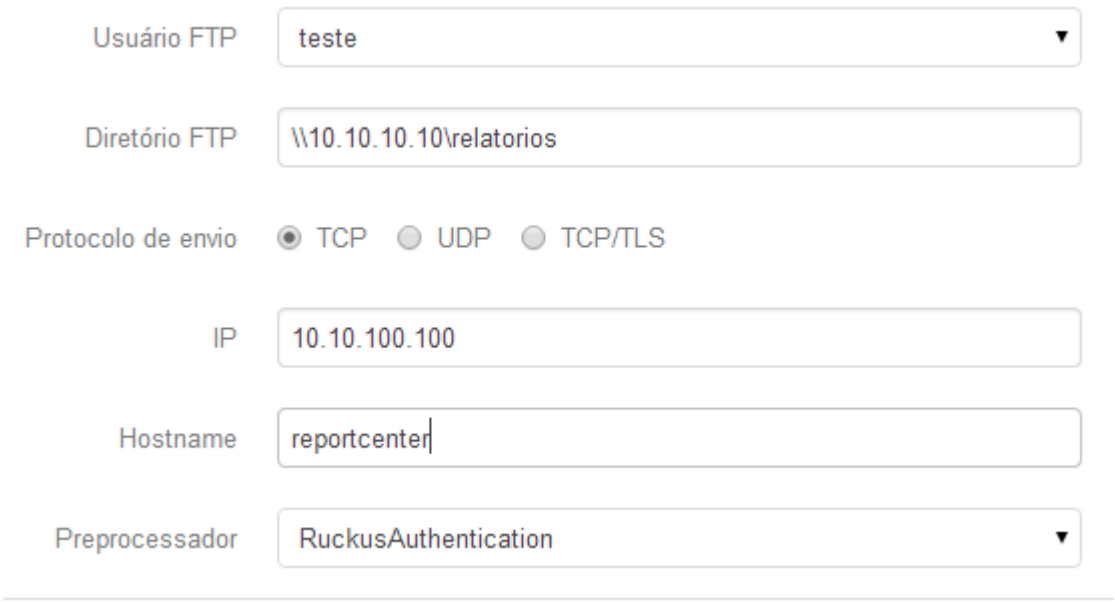


Figura 99 - Configuração de envio via FTP

Usuário FTP: Neste campo deve-se definir o usuário FTP que será usado na autenticação;

Diretório FTP: Neste campo deve-se definir o diretório FTP que armazenará os logs. Esse campo não pode ter espaços ou barras, pois é o nome de um diretório que está no Aker Report Center instalado.

Protocolo de envio: Neste campo deve-se selecionar qual o protocolo que será usado no envio, as opções disponíveis são: **TCP, UDP, TCP/TLS.**

IP: Neste campo deve-se inserir o IP da máquina a qual enviará o log.

Hostname: Neste campo deve-se inserir *hostname* da máquina a qual enviará o log (somente para identificação)

Pré-processador: Neste campo deve-se selecionar o preprocessador que irá fazer um pré-processamento nos eventos do ativo em questão.

Envio Syslog

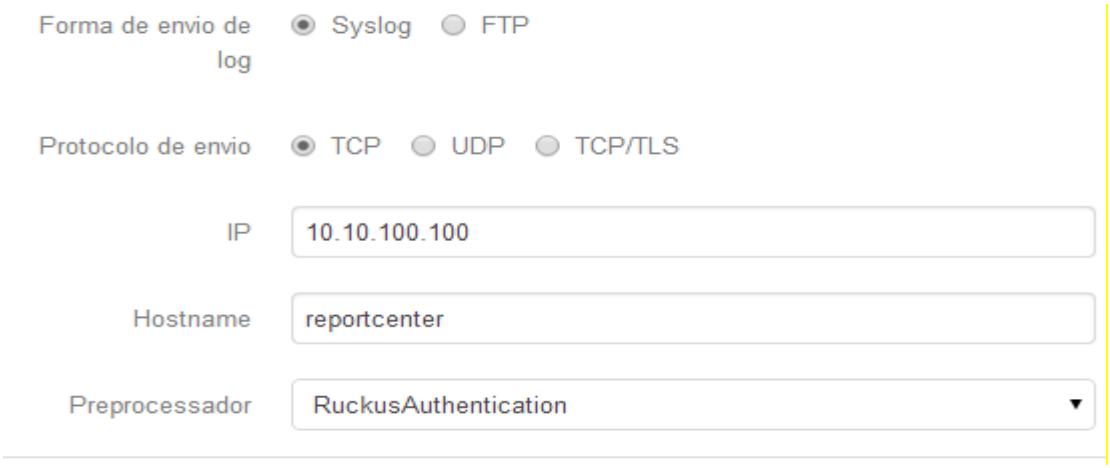


Figura 100 - Envio Syslog

Protocolo de envio: Neste campo deve-se selecionar qual o protocolo que será usado no recebimento de logs, as opções disponíveis são: **TCP, UDP, TCP/TLS.**

IP: Neste campo deve-se inserir o IP da máquina a qual enviará o log.

Hostname: Neste campo deve-se inserir *hostname* da máquina a qual enviará o log (somente para identificação).

Preprocessador: Neste campo deve-se selecionar o preprocessador que irá fazer um pré-processamento nos eventos do ativo em questão.

A quantidade de ativos é limitada pela licença do usuário.

Ao configurar um Ativo é necessário configurar o firewall em questão para que ele envie os logs para o Aker Report Center, siga os passos a seguir para fazer este procedimento no Aker Firewall:

- No firewall desejado acesse o menu “Configurações do sistema” e escolha a opção parâmetros de configuração;

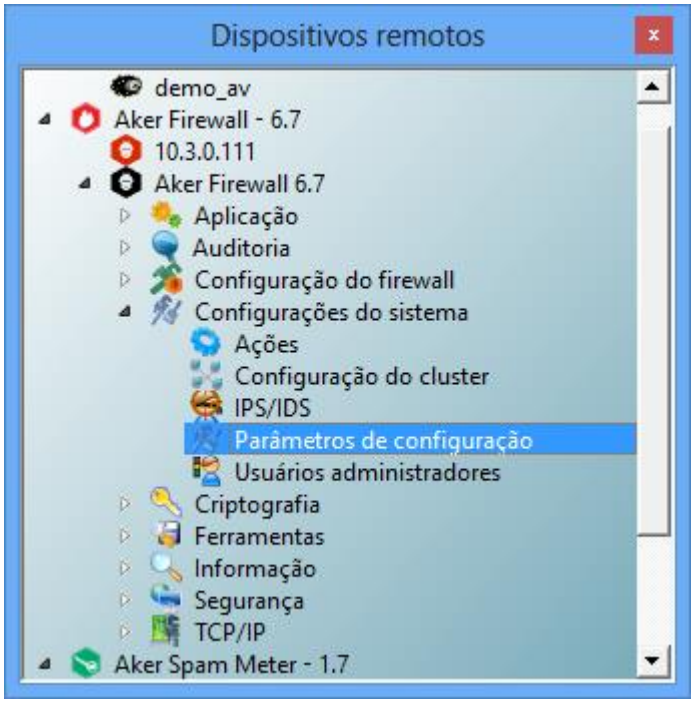


Figura 101 - Parâmetros de configuração

- Acesse a aba “Log”

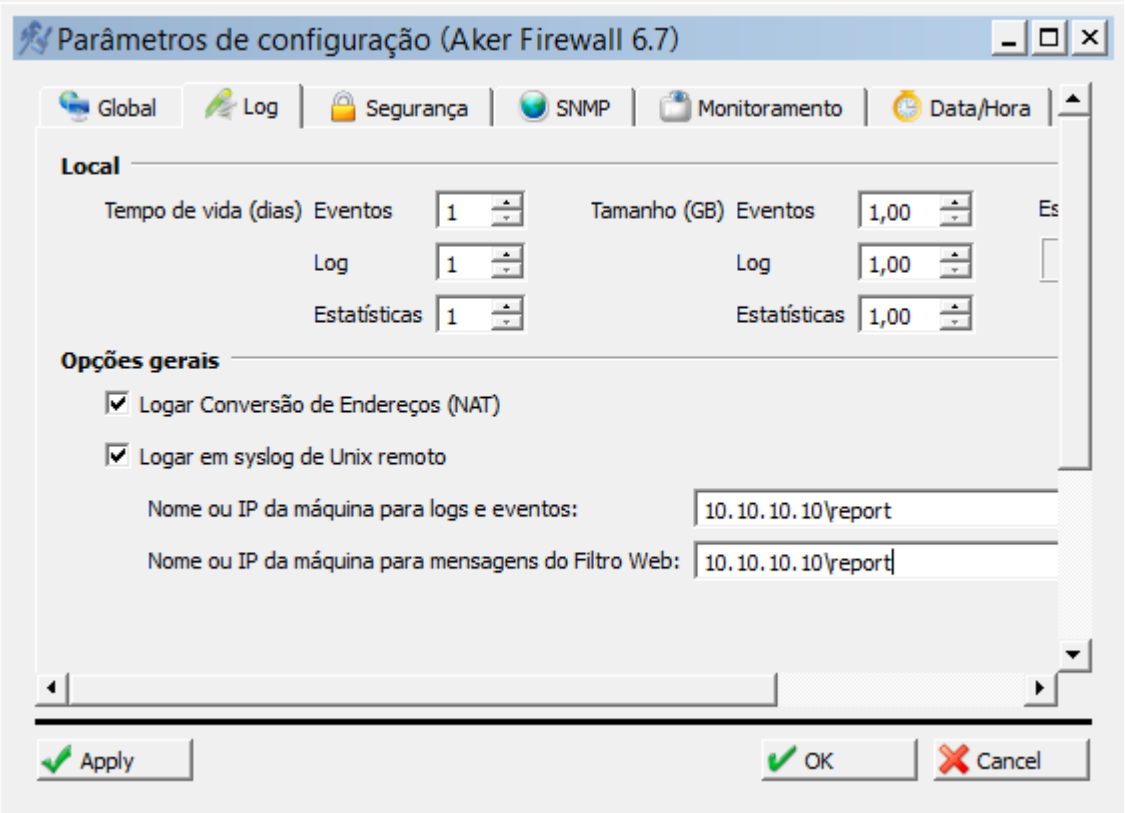


Figura 102 - Aba log

- Habilite a opção "*Logar Conversão de Endereços (NAT)* e *Logar em syslog de Unix remoto*";
- Insira o nome da máquina ou IP o qual receberá os logs, eventos e mensagens do Filtro Web, no exemplo acima foi usado "reportcenter.aker.br".
- Clique em "*OK*" para confirmar a operação;

5.2.4 Aba Eventos Processados

Esta aba exibe o número total de eventos que foram gerados pelo ativo em questão e os logs do últimos eventos processados atualizando as informações a cada 5 segundos.

Cadastro de ativo
Eventos Processados
Eventos Não Processados
Total de eventos
336.028
Últimos eventos
dst_ip: www.aker.com.br, dst_port: 80, event_type: event, src_ip: 177.69.177.57, date: 2013-11-18 15:22:33, plugin_sid: 200, username: -, userdata1: GET / HTTP/1.0, userdata2: 10543, userdata3: http://letras.mus.br/ana-carolina/258918/, userdata4: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0), filename: -, priority: notice, facility: user
dst_ip: www.aker.com.br, dst_port: 80, event_type: event, src_ip: 177.69.177.57, date: 2013-11-18 15:22:33, plugin_sid: 200, username: -, userdata1: GET / HTTP/1.0, userdata2: 10545, userdata3: http://letras.mus.br/ana-carolina/258918/, userdata4: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0), filename: -, priority: notice, facility: user
dst_ip: www.aker.com.br, dst_port: 80, event_type: event, src_ip: 177.69.177.57, date: 2013-11-18 15:22:32, plugin_sid: 200, username: -, userdata1: GET / HTTP/1.0, userdata2: 10536, userdata3: http://letras.mus.br/ana-carolina/258918/, userdata4: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0), filename: -, priority: notice, facility: user

Figura 103 - Aba Eventos processados

5.2.5 Aba Eventos Não Processados

Esta aba exibe o número total de eventos que foram gerados e o log dos últimos eventos processado pelo ativo em questão, mas não foram processados atualizando as informações a cada 5 segundos.

Aker Report Center
AKER
Cadastro de ativo
Eventos Processados
Eventos Não Processados
Total de eventos
4
Últimos eventos
Nov 18 15:23:33 www.aker.com.br: 80 177.69.177.57 - - [18/Nov/2013:15:23:33 -0200] "GET / HTTP/1.0" 200 10536 "http://ego.globo.com/famosos/noticia/2013/11/babi-rossi-sobre-affairs-de-olin-fez-cena-para-eu-ver-papel-de-crianca.html" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.57 Safari/537.36"
Nov 18 15:23:33 www.aker.com.br: 80 177.69.177.57 - - [18/Nov/2013:15:23:33 -0200] "GET / HTTP/1.0" 200 10547 "http://letras.mus.br/luan-santana/ce-topa/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.57 Safari/537.36"
Nov 18 15:23:33 www.aker.com.br: 80 177.69.177.57 - - [18/Nov/2013:15:23:32 -0200] "GET / HTTP/1.0" 200 10539 "http://letras.mus.br/ana-carolina/258918/" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0)"
Nov 18 15:23:33 www.aker.com.br: 80 177.69.177.57 - - [18/Nov/2013:15:23:32 -0200] "GET / HTTP/1.0" 200 10540 "http://letras.mus.br/ana-carolina/258918/" "Mozilla/5.0 (compatible; MSIE 9.0; Windows

Figura 104 - Aba Eventos não processados

5.2.6 Colunas

Esta opção permite que o usuário crie modelos de colunas personalizados para serem usados na criação de relatórios.

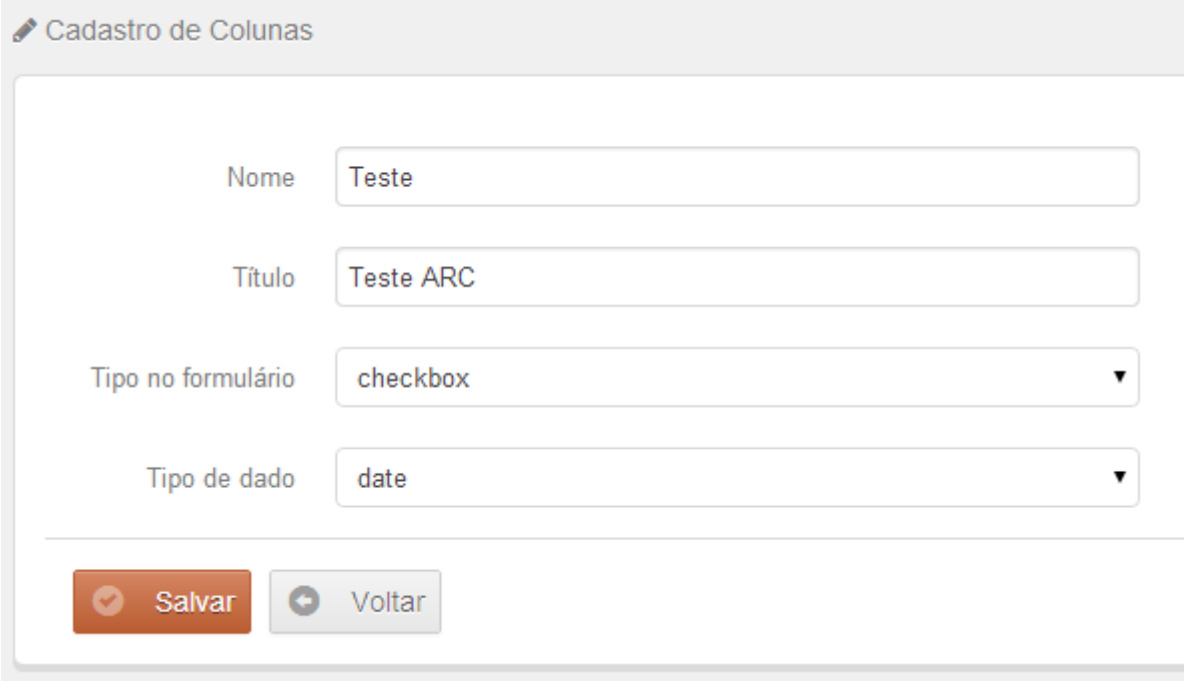


Figura 105 - Colunas

Nome: Neste campo deve-se definir o nome da coluna em criação;

Título: Neste campo deve-se definir o título da coluna em criação;

Tipo no formulário: Neste campo deve selecionar o tipo do formulário para a coluna em criação, as opções disponíveis são:

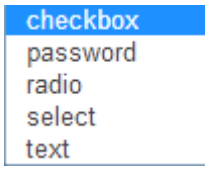


Figura 106 - Opções de colunas

Tipo de dado: Neste campo deve-se selecionar o tipo de dado para esta coluna, as opções disponíveis são:

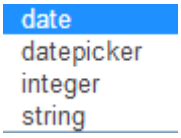


Figura 107 - Opções de tipos de dados

5.2.7 Tipos de ativo

Na janela "***Tipos de ativo***" é possível que o usuário visualize, edite, exclua ou adicione um novo tipo de ativo no sistema do Aker Report Center. Atualmente o Aker Report Center fornece 370 tipos de ativos para seus usuários.

Figura 108 - Tipos de ativos

A seguir detalhes sobre como adicionar um novo tipo de ativo.

5.2.8 Adicionando um novo tipo de ativo:

Para adicionar um novo tipo de ativo siga os passos a seguir:

- Clique em

para que a janela de cadastro a seguir seja exibida:

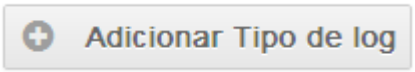
Figura 109 - Adicionando um novo tipo de ativo

- Preencha os campos de janela de cadastro de tipo de ativo corretamente:

Nome: Neste campo deve-se inserir o nome do novo tipo de ativo (ex: Aker Firewall 6.7)

Descrição: Neste campo deve-se inserir uma descrição para o novo tipo de ativos (ex: logs Aker Firewall 6.7).

Fabricantes: Neste campo deve-se inserir o nome do fabricante (ex: Aker Security Solutions)

Ao preencher os campos acima corretamente clique em 

, para configurar os tipos de log que serão registrados.

A janela a seguir será exibida:

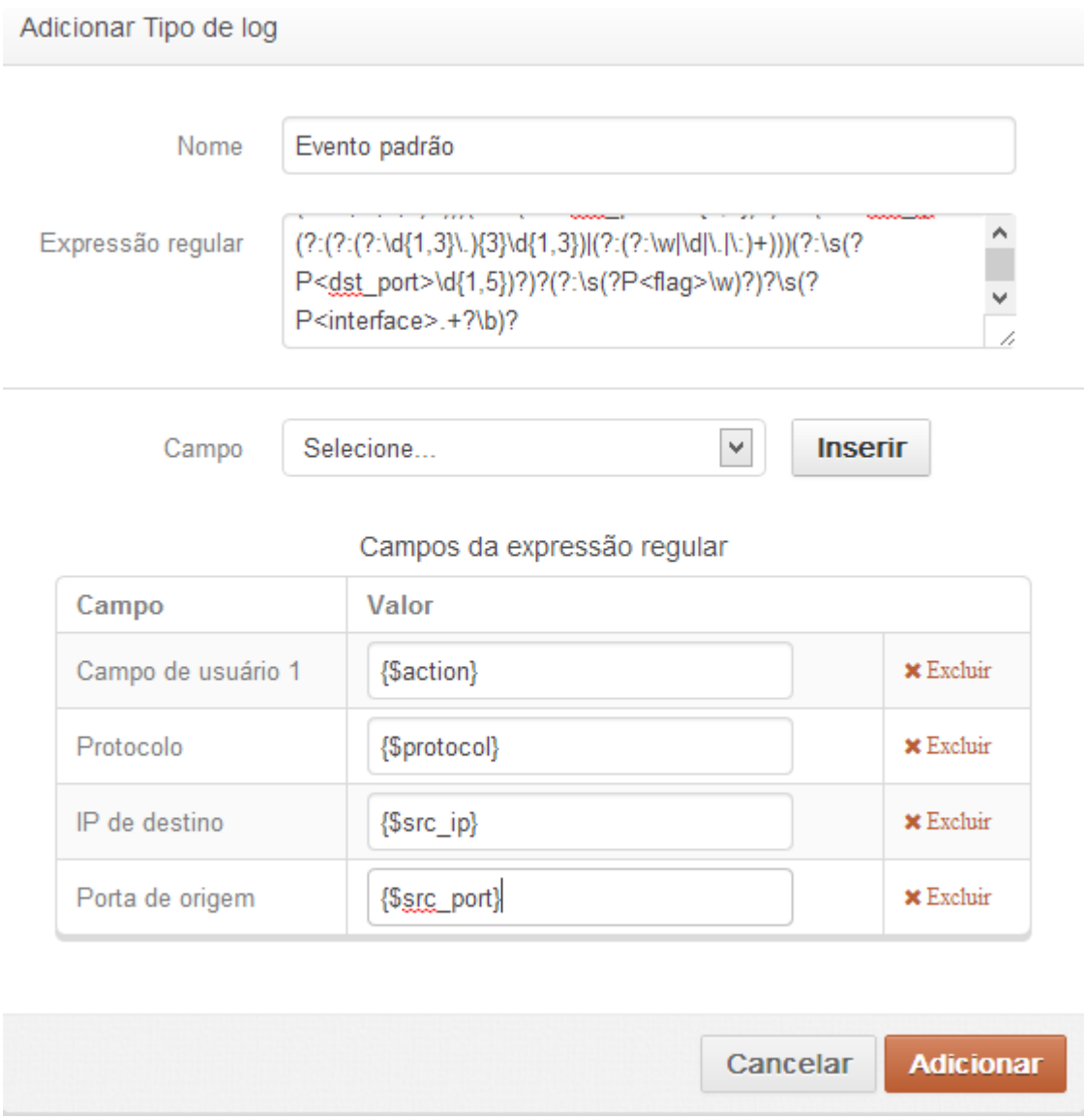


Figura 110 - Adicionando um novo tipo de log

Nome: Neste campo deve-se inserir o nome do tipo de log que será cadastrado (ex: *Evento padrão*).

Expressão regular: Neste campo deve-se inserir a expressão regular, como no exemplo abaixo:

Aker_Firewall\:\s(?P<action>[ACDR])\s(?P<protocol>\w+)\s(?P<src_ip>(?:(?:(?:\d{1,3}\.){3}\d{1,3})|(?:(?:\w|\d|\.|\:)+)))(?:\s(?P<src_port>\d{1,5})?)?\s(?P<dst_ip>(?:(?:(?:\d{1,3}\.){3}\d{1,3})|(?:(?:\w|\d|\.|\:)+)))(?:\s(?P<dst_port>\d{1,5})?)?(?:\s(?P<flag>\w)?)?\s(?P<interface>.+?\b)?

Campo: Nessa opção deve-se selecionar os campos que serão usados no armazenamento dos logs.

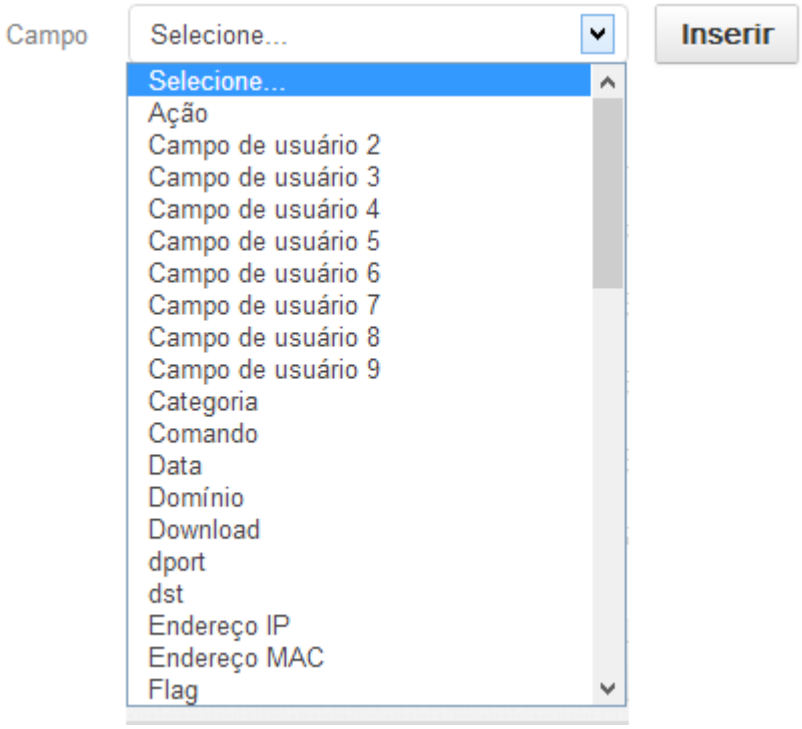


Figura 111 - Seleção de campos

Ao selecionar o campo, é necessário que o usuário clique em "Inserir" para que o campo abaixo seja exibido.

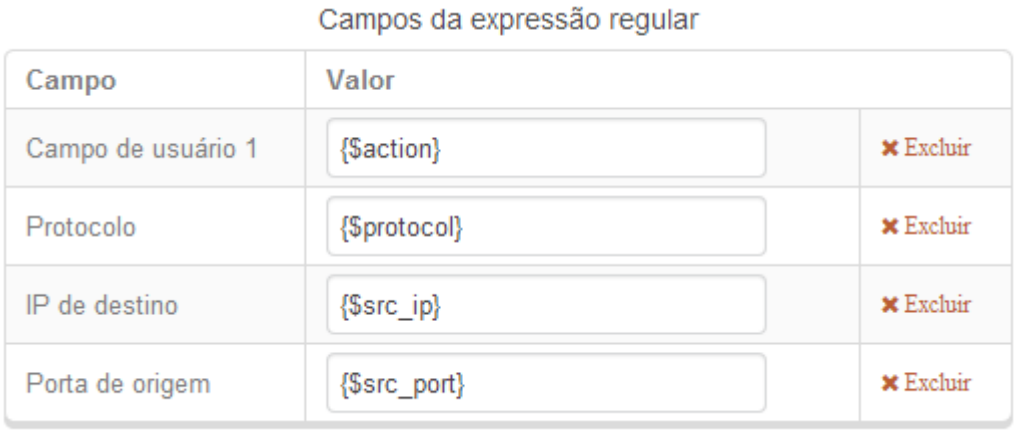


Figura 112 - Campo de expressões regulares

Na listagem de expressões regulares acima, é necessário que o campo "***Valor***" seja preenchido corretamente para que o match seja feito (ou seja, o processo que irá validar as informações, por exemplo, o campo "PROTOCOLO refere-se à ***{$procol}*** na expressão).

- Clique em

, para concluir o cadastro.

5.3 *Relatórios*

O submenu "*Relatórios*" permite o usuário configure os padrões de exportação de dados e a personalização da logo que será exibida nos relatórios.

5.3.1 Customização

O menu "***Customização***" permite que o usuário personalize a logo do exibida nos relatórios do Aker Report Center.

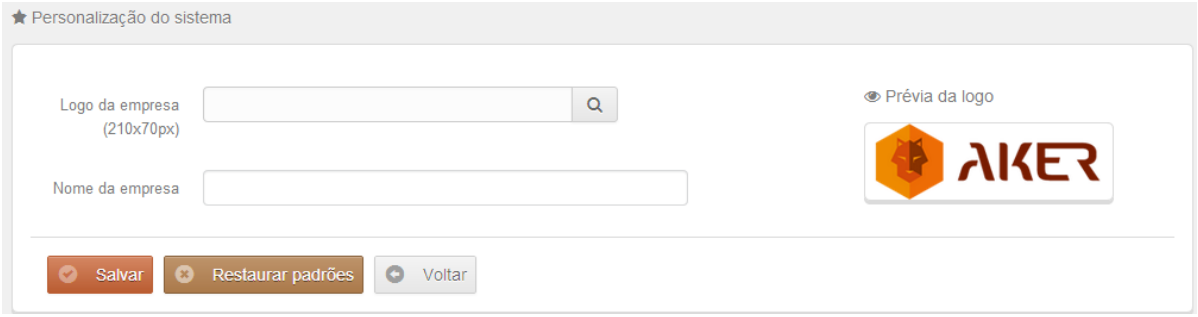


Figura 113 - Personalização do sistema

5.3.2 Preferências de exportação de dados

Na janela "***Preferência de Exportação de dados***" o usuário deve definir os padrões que serão usados na exportação dos relatórios em formato **TXT**.

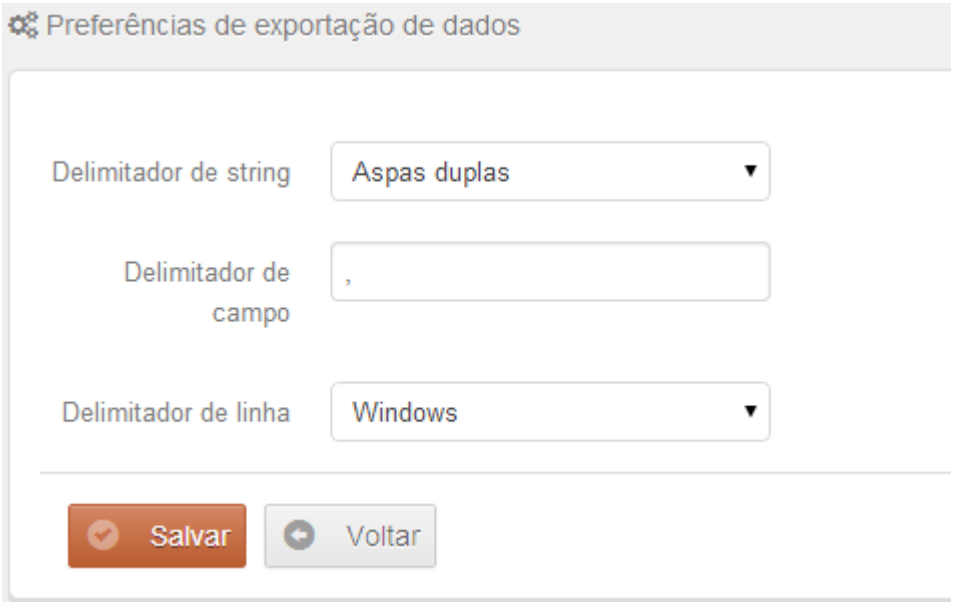


Figura 114 - Preferências de exportação de dados

5.4 Segurança

O submenu "***Segurança***" permite que o usuário defina as configurações FTP/TLS, Syslog TLS, configurações dos usuários FTP, e perfis de usuários.

5.4.1 Perfis

Na janela "***Perfis***" é possível visualizar todos os perfis usuários existentes no sistema, e também editar, excluir e adicionar um novo perfil de usuário no sistema.

Figura 115 - Janela Perfis

5.4.2 Usuários

Na janela "***Usuários***" é possível visualizar todos os perfis de usuários existentes no sistema, e também editar, excluir, e adicionar um novo usuário no sistema.

Figura 116 - Usuários

5.4.1 Configurações FTP TLS

Na janela "***Configuração FTP/TLS***" deve-se definir se a conexão segura será usada ou não para os usuários que serão logados via FTP. Caso escolha "***Sim***" o usuário deve definir se

a conexão TLS será obrigatória ou não, ao selecionar "**Sim**" apenas conexões TLS serão permitidas e selecionando "**Não**" conexões TLS e FTP serão permitidas. Nesta janela também é possível carregar a chave e o certificado do servidor que serão usados para criptografar a conexão.

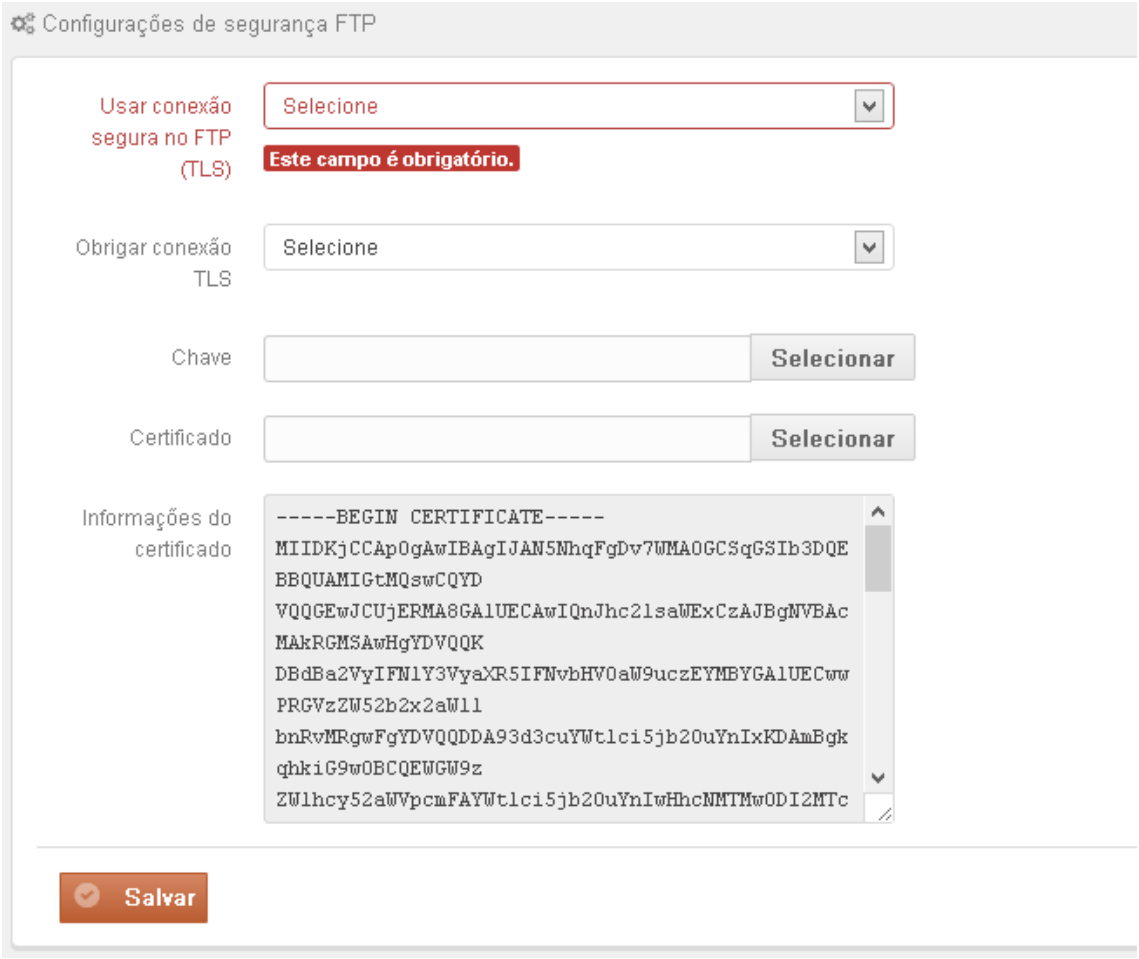


Figura 117 - Configuração de segurança FTP

5.4.2 Syslog TLS

Na janela "***Syslog TLS***" define-se como os logs serão aceitos, apenas criptografados de conexões confiáveis, ou serão aceitos logs de qualquer conexão.

Ao selecionar "**Sim**" conexões não confiáveis serão aceitas, e selecionando "**Não"** os campos da janela abaixo serão exibidos:

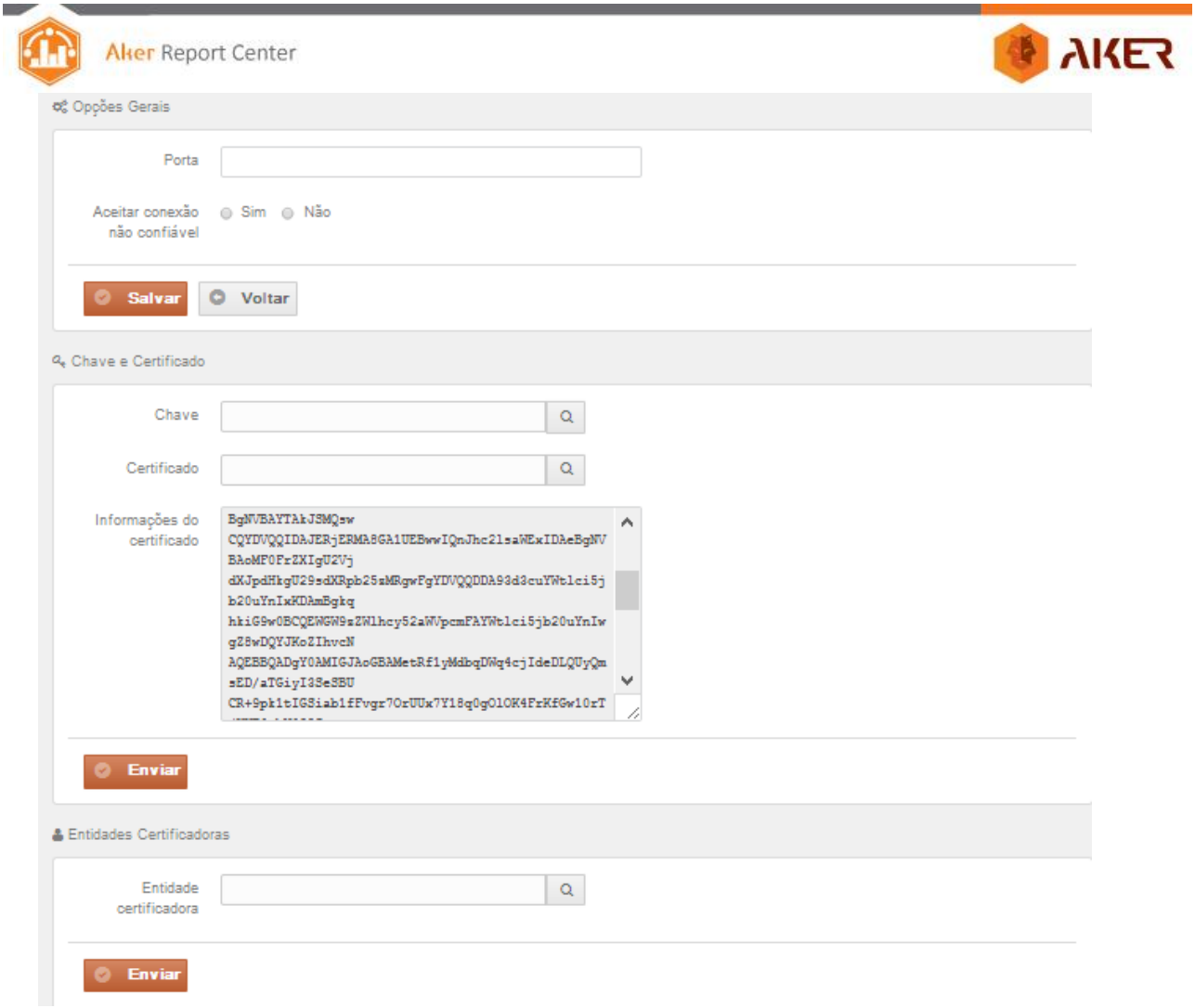


Figura 118 - Syslog TLS

5.4.3 Usuários FTP

Na janela "***Usuários FTP***" o administrador pode visualizar os usuários FTP cadastrados no sistema, editar, deletar ou adicionar novos usuários FTP.

Figura 119 - Usuários FTP

Para cadastrar um novo usuário FTP siga os passos abaixo:

- Na janela de usuários FTP clique em + Adicionar, para que a janela abaixo seja exibida:

Figura 120 - Cadastro de usuário FTP

- Insira o nome do novo usuário e sua respectiva senha, e então clique em Salvar para finalizar o cadastro do novo usuário FTP.

5.4.4 Tipo de autenticação

Na aba "***Tipo de autenticação***" o usuário deve selecionar qual o tipo de autenticação que será efetuada:

- **Não**: Ao selecionar "*Não*" a autenticação será feita por meio de uma base local (banco de dados do sistema).
- **Sim**: Ao selecionar "*Sim*" a autenticação será feita por meio de uma base LDAP.

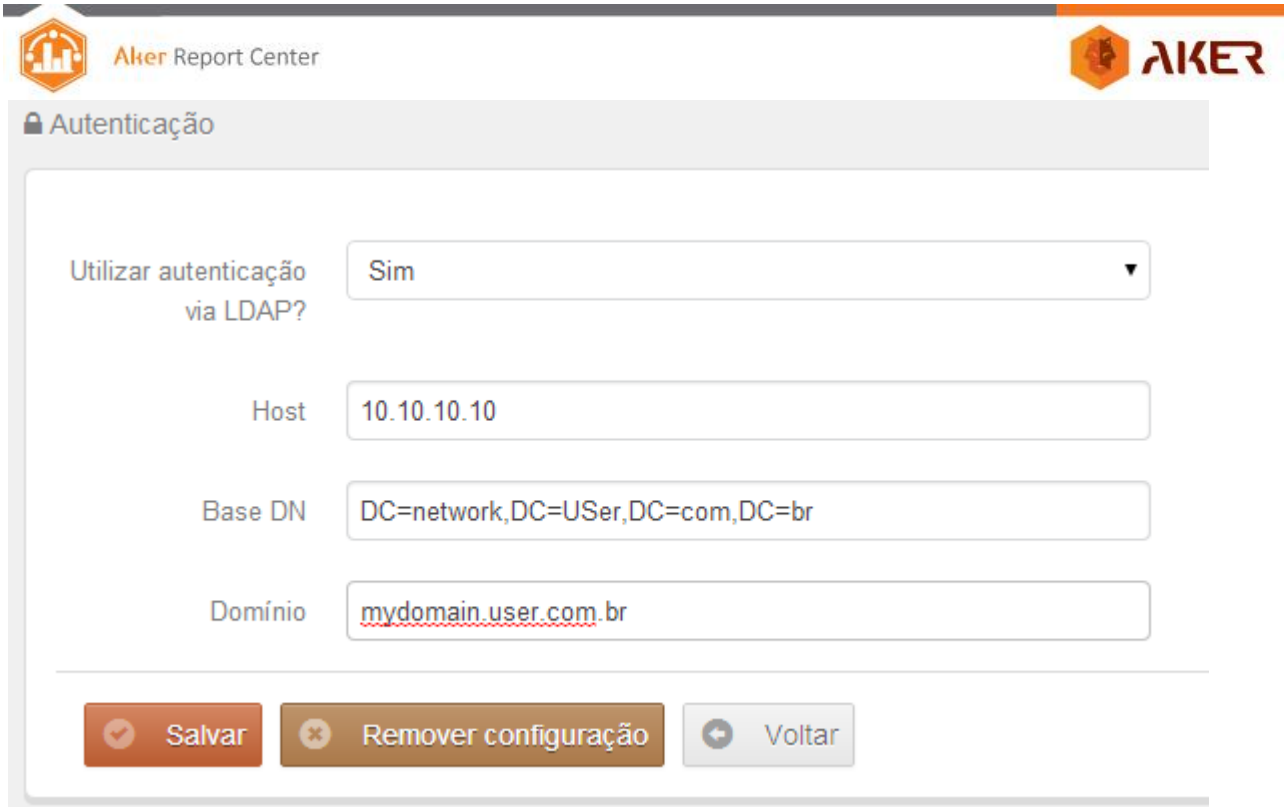


Figura 121 - Autenticação

5.5 *Rede*

Este submenu permite que o usuário configure a interface de rede do Aker Report Center e o Servidor NTP.

5.5.1 Interfaces de rede

Na janela "***Interfaces de rede***" o usuário pode configurar as interfaces de rede da máquina que o Aker Report Center está instalado.

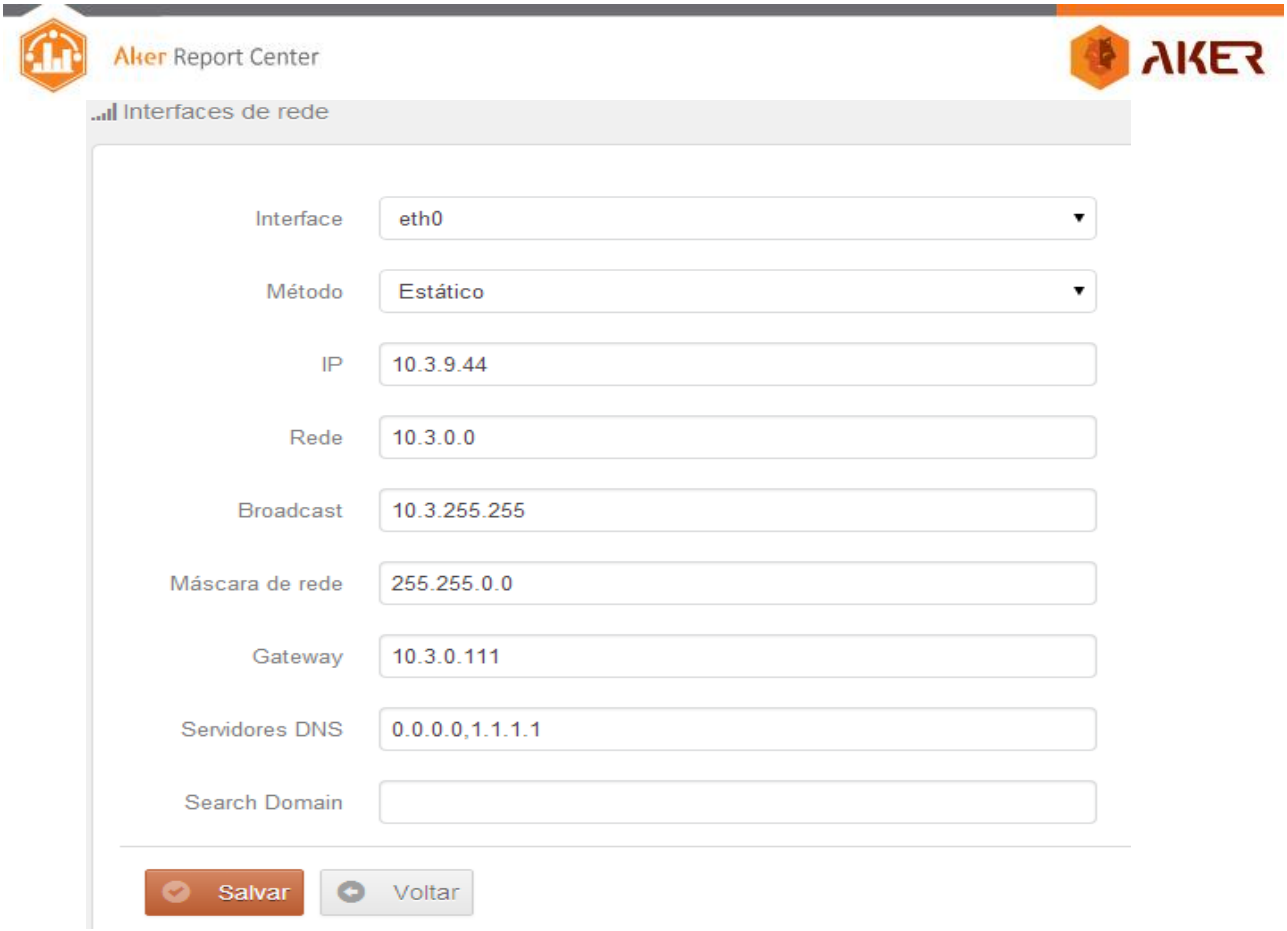


Figura 122 - Janela de configuração de rede

Interface: Neste campo o usuário deve selecionar a interface de rede que será configurada para o Aker Report Center;

Método: O Aker Report Center oferece dois métodos de configuração de redes para seus usuários que são:

- **DHCP** – para usar este método o usuário deve ter um servidor DHCP na rede para pegar o IP manualmente.
- **Estático** – ao selecionar este método o usuário deve configurar a rede manualmente preenchendo os dados a seguir:

IP: Neste campo o usuário deve definir o IP do ARC;

Rede: Neste campo o usuário deve definir o IP da rede do usuário;

Broadcast: Neste campo o usuário deve definir o IP de broadcast;

Máscara de rede: Neste campo o usuário deve definir máscara de rede em uso;

Gateway: Neste campo o usuário deve inserir o gateway da rede;

Servidor DNS: Neste campo o usuário pode inserir o servidor de DNS da rede do usuário. Para inserir um DNS secundário insira uma virgula (,) entre **os endereços DNS**

Exemplo: 10.0.0.150,10.0.0.200

5.5.2 Servidores NTP

Na janela "**Servidores NTP – Network Time Protocol**" o usuário configura os servidores NTP que serão usados para sincronizar a hora do servidor mantendo a mesma sempre exata.

Apenas os servidores da http://www.pool.ntp.org/en/ são aceitos.

Figura 123 - Servidores NTP

5.6 *Backup*

O submenu "***Backup***" permite que o usuário faça um backup de suas configurações ou carregue um backup que foi salvo previamente. Este submenu possui duas opções que serão abordadas a seguir:

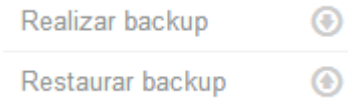


Figura 124 - Opções de backup

5.6.1 Realizar backup

A opção "***Realizar backup***" permite que o usuário salve um backup das configurações do Aker Report Center em questão. Para fazer o backup das configurações do Aker Report Center simplesmente clique em

.

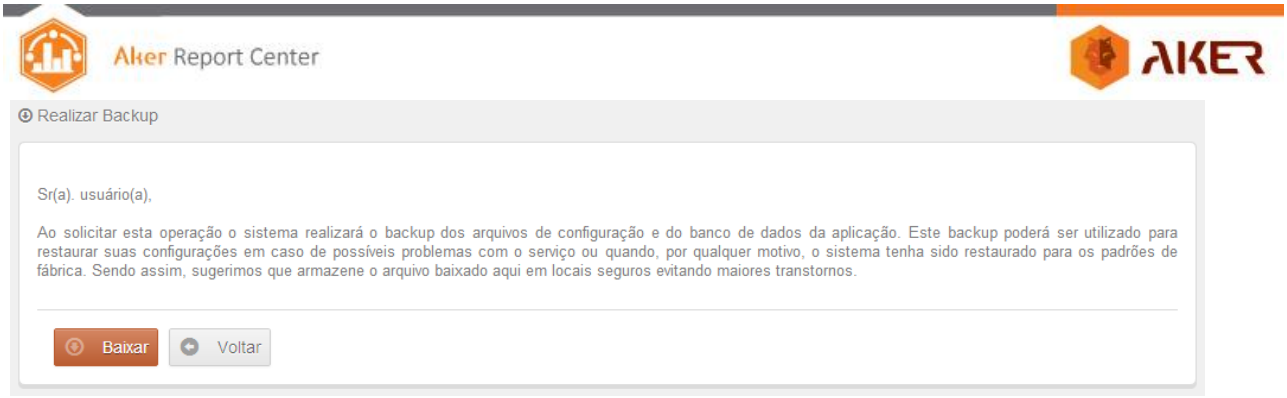

Aker Report Center
AKER
Realizar Backup
Sr(a). usuário(a),
Ao solicitar esta operação o sistema realizará o backup dos arquivos de configuração e do banco de dados da aplicação. Este backup poderá ser utilizado para restaurar suas configurações em caso de possíveis problemas com o serviço ou quando, por qualquer motivo, o sistema tenha sido restaurado para os padrões de fábrica. Sendo assim, sugerimos que armazene o arquivo baixado aqui em locais seguros evitando maiores transtornos.
Baixar
Voltar

Figura 125 - Janela Realizar Backup

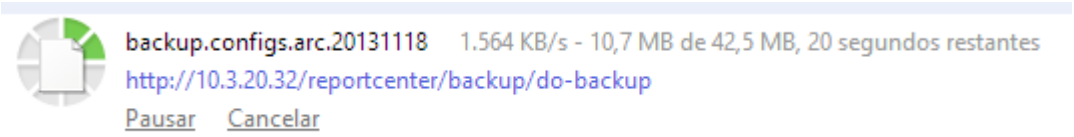

backup.configs.arc.20131118 1.564 KB/s - 10,7 MB de 42,5 MB, 20 segundos restantes
http://10.3.20.32/reportcenter/backup/do-backup
Pausar Cancelar

Figura 126 - Criação de backup

5.6.2 Restaurar backup

A janela "***Restaurar backup***" permite que o usuário restaure as configurações do Aker Report Center através de um backup previamente salvo.

Este procedimento excluirá toda e qualquer informação contidas nas configurações em uso, salvando apenas as configurações do backup.

Para restaurar um backup siga os passos a seguir:

- Clique no botão .
- Localize o arquivo para que será usado para restaurar as configurações do Aker Report Center.

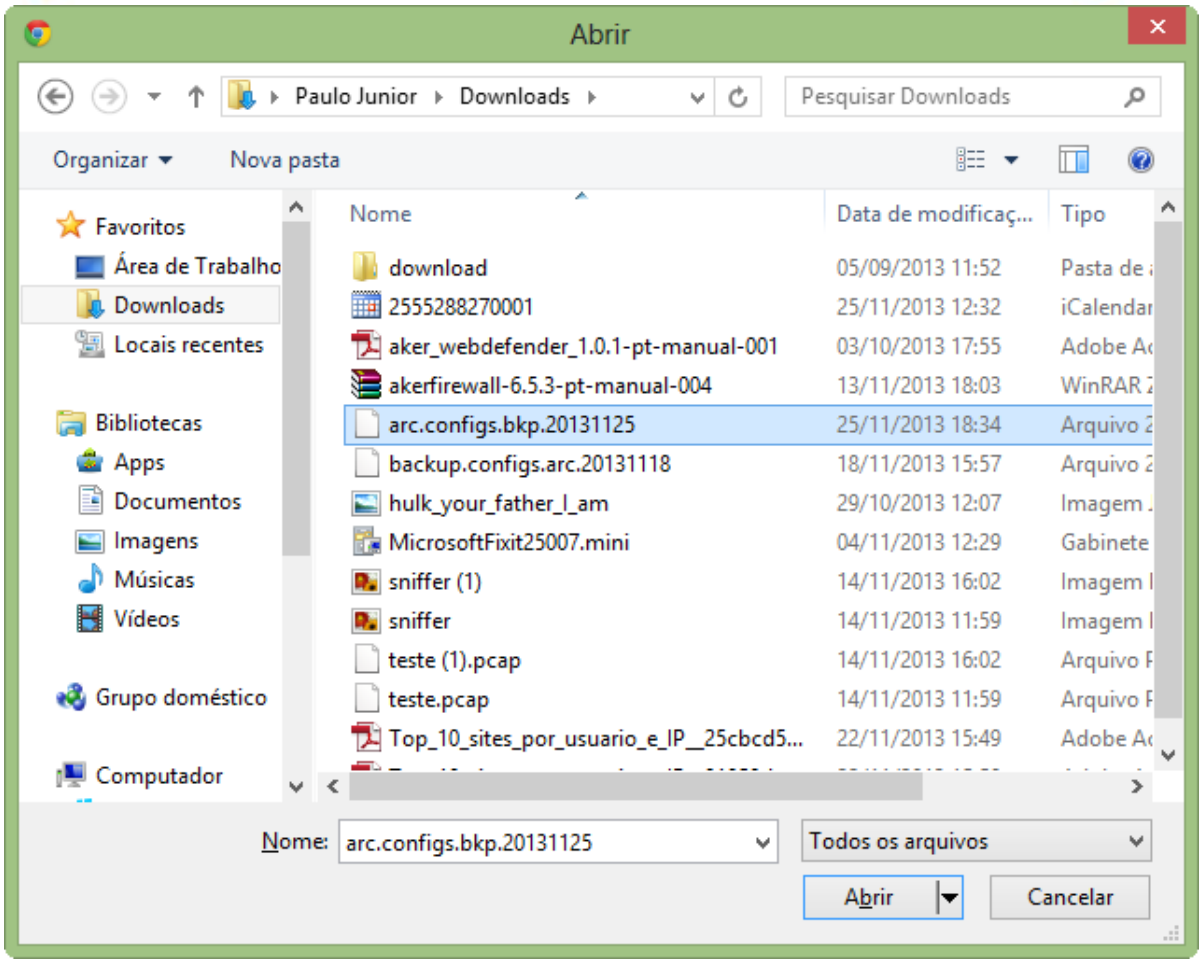


Figura 127 - localizando arquivo de backup

➢ Clique em

.

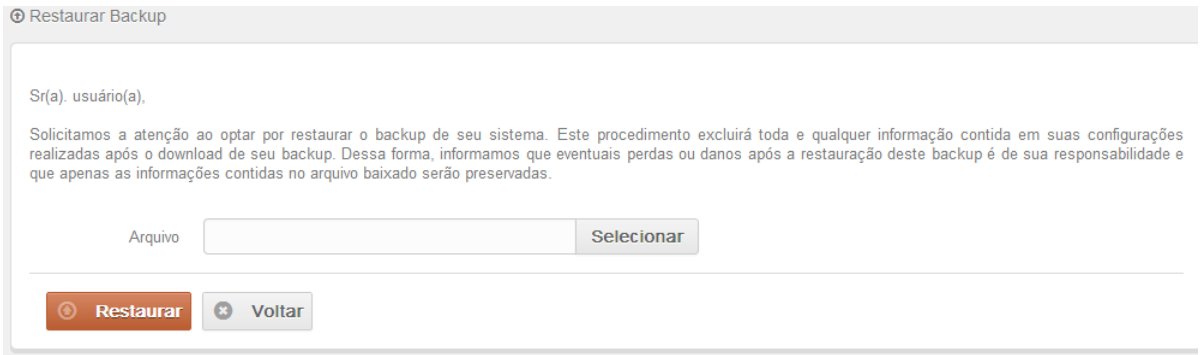

Restaurar Backup
Sr(a). usuário(a),
Solicitamos a atenção ao optar por restaurar o backup de seu sistema. Este procedimento excluirá toda e qualquer informação contida em suas configurações realizadas após o download de seu backup. Dessa forma, informamos que eventuais perdas ou danos após a restauração deste backup é de sua responsabilidade e que apenas as informações contidas no arquivo baixado serão preservadas.
Arquivo
Selecionar
Restaurar
Voltar

Figura 128 - Janela Restaurar Backup

5.7 Licenciamento

Este submenu permite que o usuário configure os parâmetros de sua licença. Ao terminar a instalação do sistema, no primeiro login o usuário deve gerar a chave de licenciamento do produto. Ao gerar a chave de licenciamento o usuário deve enviar a mesma, juntamente com o nome o qual a chave foi licenciada para licenca@aker.com.br solicitando sua licença.

5.7.1 Gerar Chave

Para gerar a chave de licenciamento do produto e carregar a licença do produto siga os passos abaixo:

- Preencha os dados da janela abaixo corretamente e clique em

.

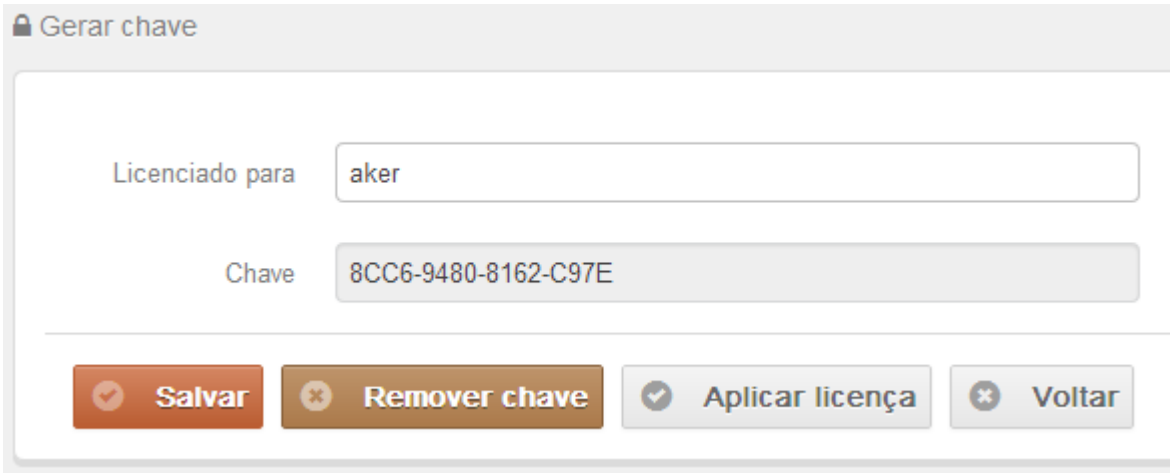


Figura 129 - Gerar chave

Licenciando para: Neste campo deve-se informar o nome do usuário ou empresa para qual o produto está sendo licenciado.

Chave: Ao preencher o campo acima a chave de licenciamento será gerada automaticamente, o usuário deve encaminha está chave para licenca@aker.com.br solicitando sua licença, ao receber a licença siga os passos a seguir (*ao enviar a solicitação o usuário receberá sua licença no período máximo de 24h*).

5.7.2 Aplicar Licença

Esta janela permite que o usuário aplique a licença gerada pela Aker.

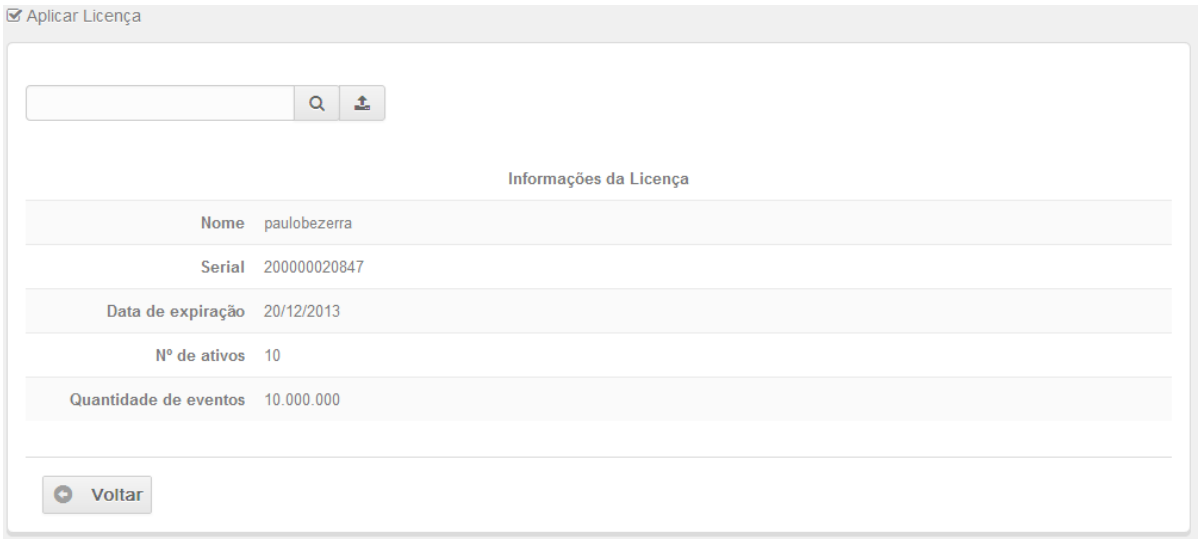


Figura 130 - Aplicar licença

Para aplicar a licença siga os passo a seguir:

- Ao receber a licença clique em

- Na janela Aplicar Licença clique no ícone para localizar sua licença.

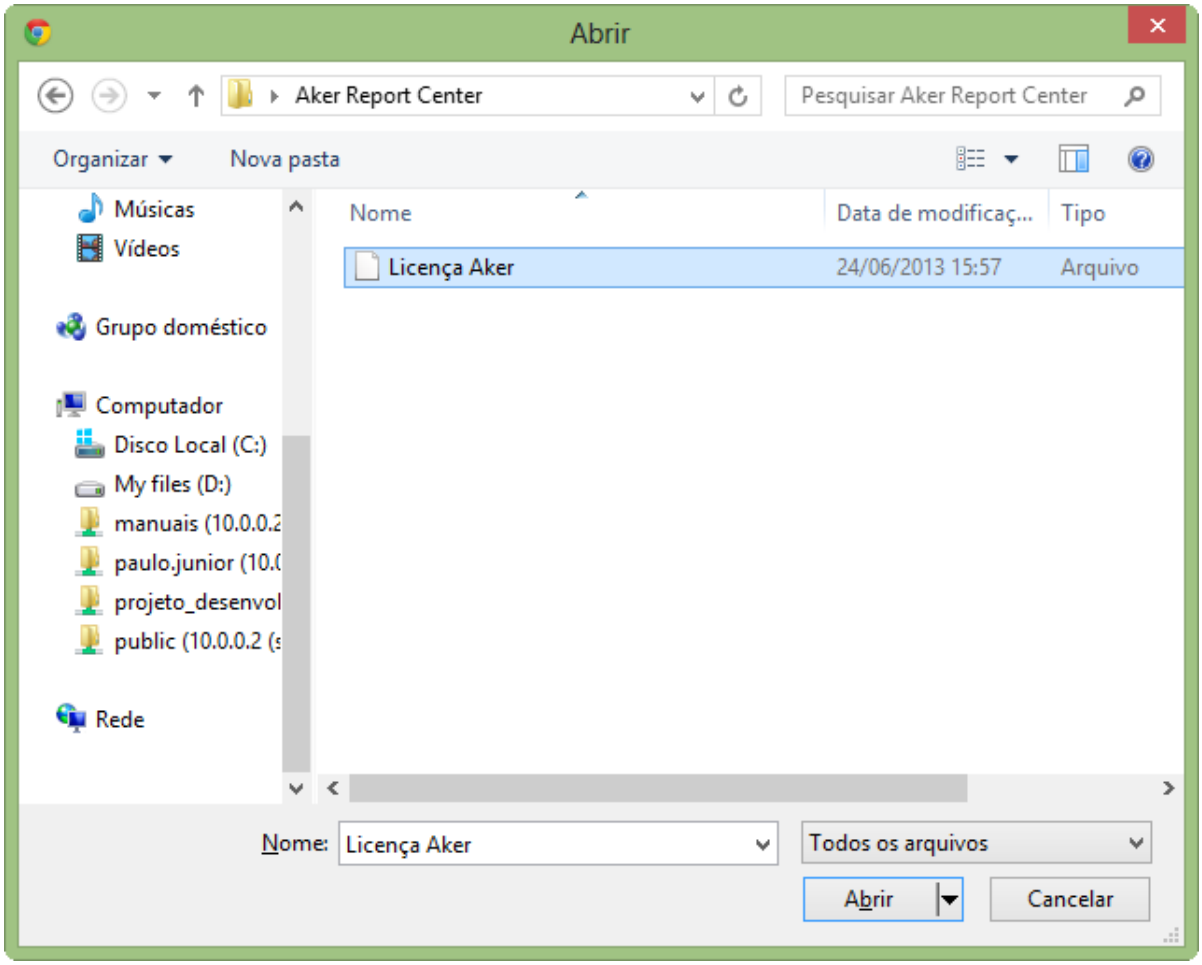


Figura 131 - Localizando licença

Figura 132 - Opções para carregar licença

- Ao localizar o arquivo clique em para carregar o arquivo;

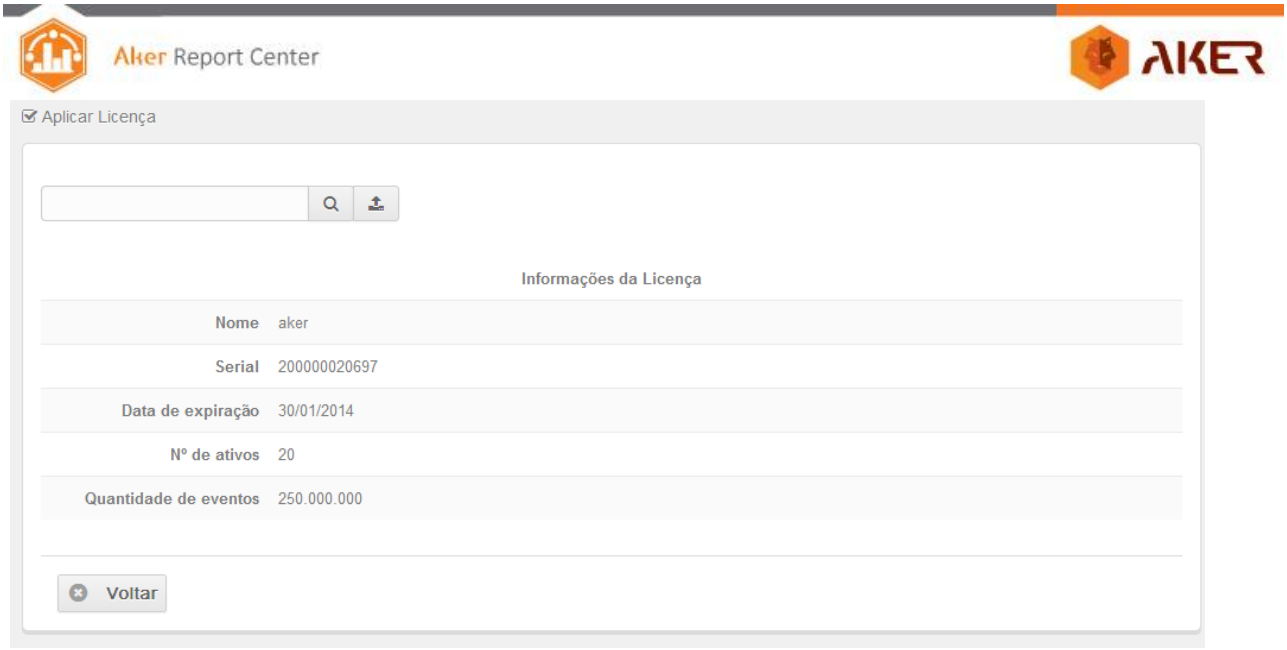


Figura 133 - Informações da licença após aplicada

Depois de completar o processo de upload da licença no sistema, será exibido as informações da licença, clique no botão

depois do upload para completar processo de licenciamento .

5.8 Outras Configurações

Este submenu permite que o usuário configures as configurações de exportação de dados, Rotate, Atualização, e-mail, e outros serviços.

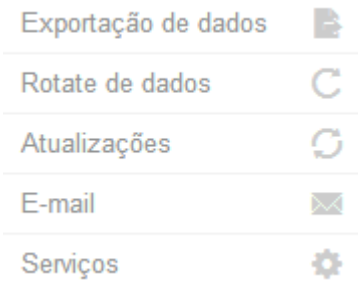


Figura 134 - Outras configurações

5.8.1 Exportação de dados

Nesta janela é possível que o usuário configure seu *Aker Report Center* para enviar seus dados para outro *Aker Report Center,* por exemplo, o *Aker Report Center* de uma ou várias *filiais* enviando seus dados para uma *Matriz* possibilitando o gerenciamento centralizado dos ativos como exibido no exemplo abaixo:

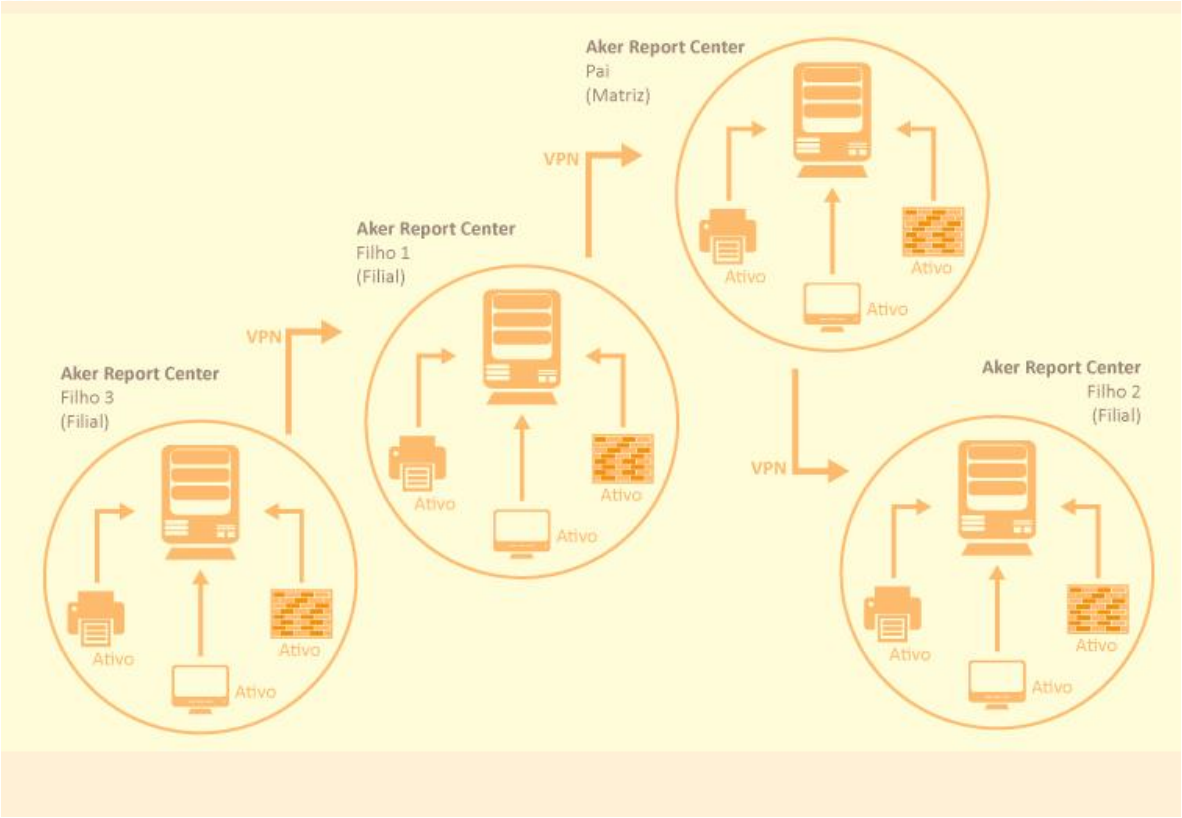


Figura 135 - Esquema de exportação de dados

Neste exemplo os Aker Report Centers filhos 1, 2, e 3 estão enviando os dados (logs, eventos, etc.) de seus ativos via FTP para o Aker Report Center da Matriz, possibilitando um gerenciamento de dados centralizado na matriz.

A seguir detalhes da janela de agendamento de exportação de dados:

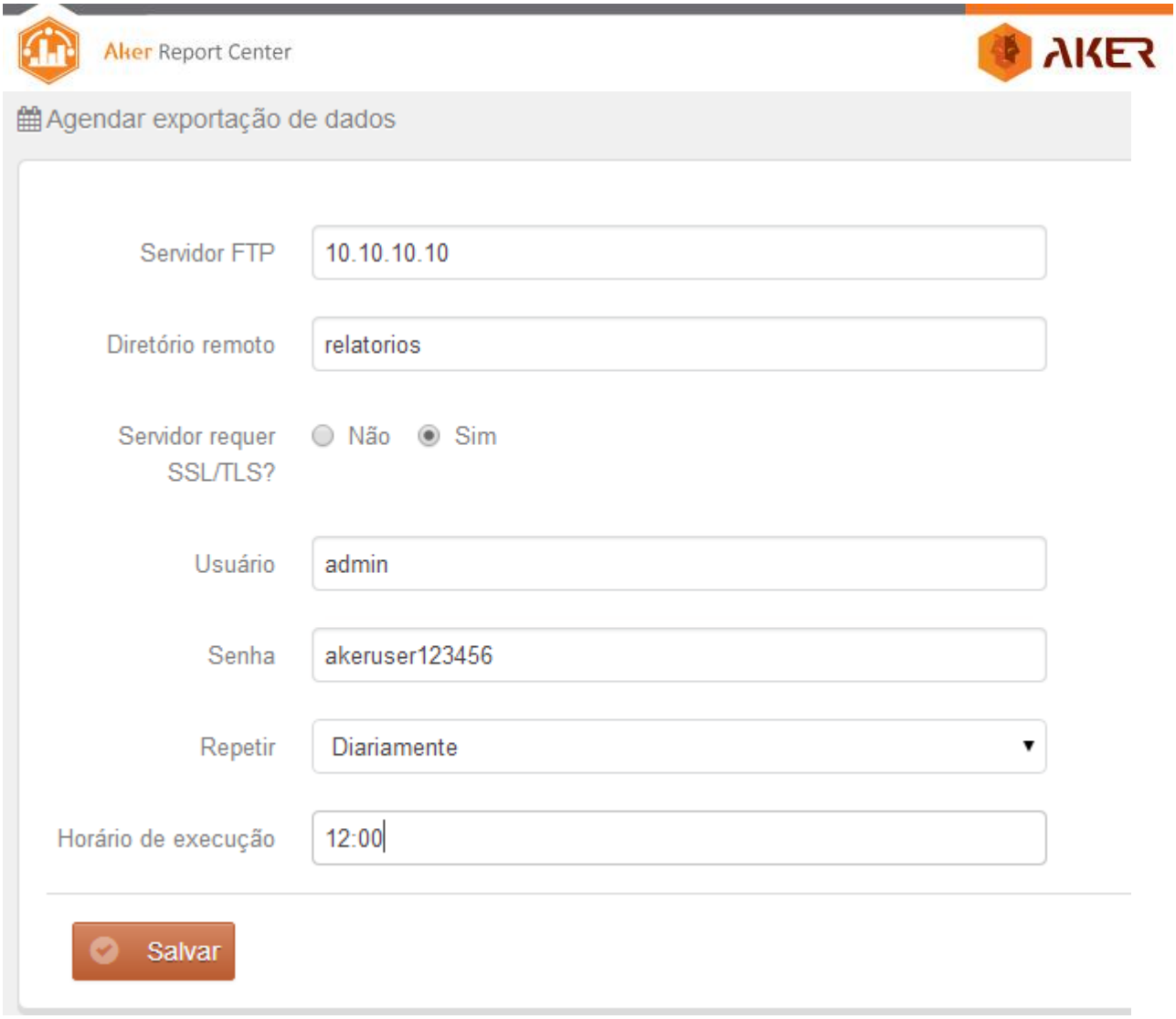


Figura 136 - Janela Agendar exportação de dados

Servidor FTP: Neste campo o usuário deve inserir o caminho do servidor que irá receber os dados;

Diretório remoto: Neste campo o usuário deve inserir o diretório remoto usado na conexão FTP. Este diretório deve ser o mesmo especificado na criação do ativo (*Menu Configurações – Ativos – Cadastro de Ativos*) o qual está exportando os *Configurações – Ativos – Cadastro de Ativos*) o qual está exportando os relatórios.

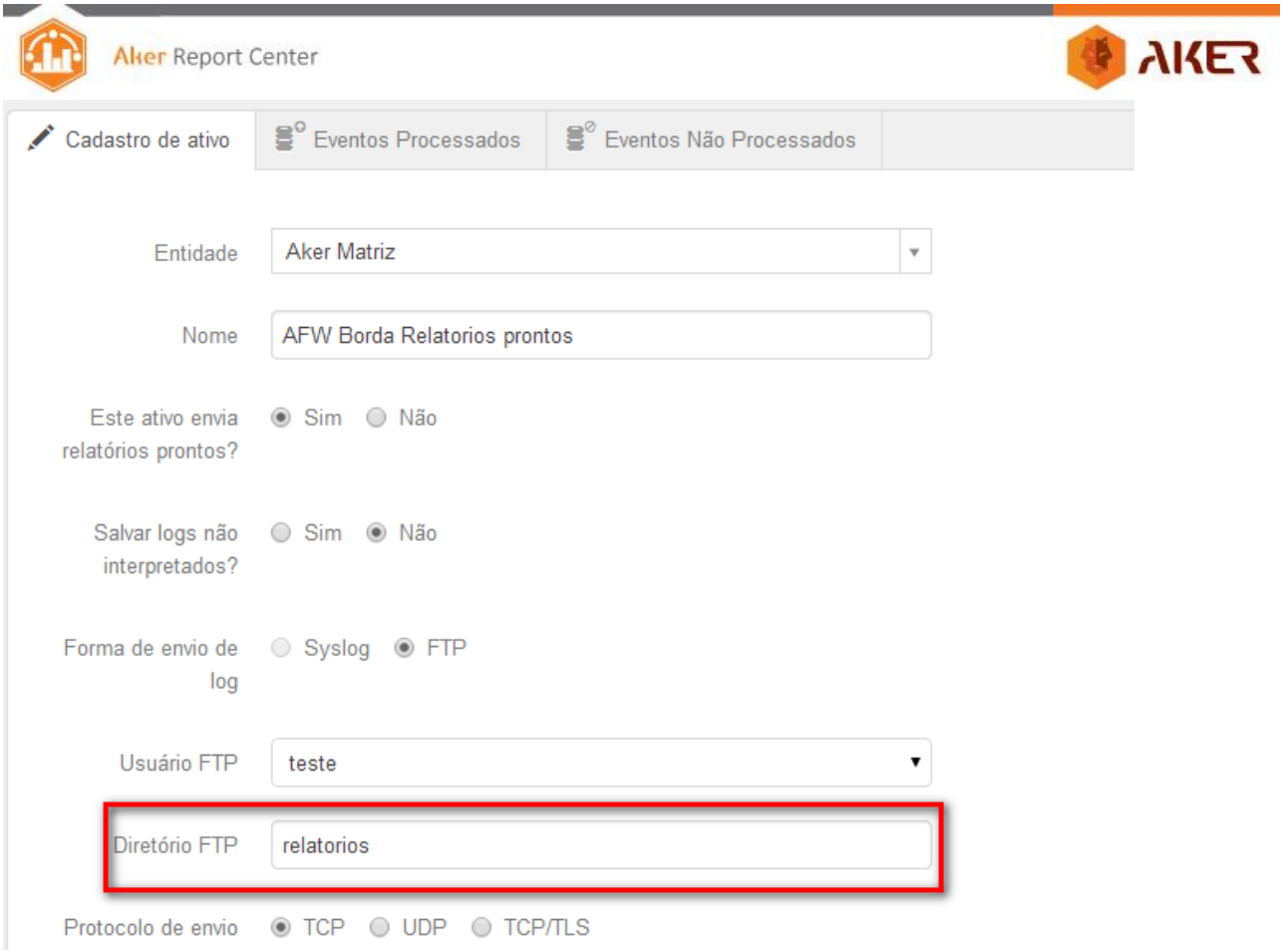


Figura 137 - Janela de cadastro de ativo

Servidor Requer SSL/TLS: Neste campo o usuário deve definir se o servidor irá ou não, solicitar uma conexão SSL/TLS para autenticação;

Usuário: Nome do usuário que será usado na autenticação;

Senha: Senha usada para autenticar o usuário;

Repetir: Neste campo o usuário deve definir a frequência que a exportação de dados será feita, as opções disponíveis são: *Diariamente, Semanalmente ou Mensalmente*;

Horário de execução: Neste campo o usuário deve selecionar o horário que a exportação será feita;

5.8.2 Rotate

Na janela "***Rotate***" o usuário pode definir as configurações de armazenamento dos logs, a quantidade de dias que os registros serão mantidos no servidor, se os registros excluídos serão salvos em um diretório ou não, por quando tempo os backups serão mantidos e o tamanho máximo do diretório que armazenará os backups.

Figura 138 - Rotate

Manter Registros por quantos dias: Neste campo o usuário deve definir a quantidade de dias que os registros serão mantidos no banco de dados;
Fazer backup de registros excluídos: Neste campo o usuário deve definir se um backup dos registros excluídos será feito ou não. Caso selecione a opção "**Sim**" as opções a seguir serão exibidas;
Manter backup por quantos dias: Neste campo o usuário deve definir a quantidades de dias que o backup de registros excluídos será mantido no sistema;
Tamanho máx. do diretório de backup (MB): Neste campo o usuário deve definir o tamanho máximo que será usado do diretório de backup para armazenar os registros excluídos.

Todos os registros enviados para o diretório de backup serão salvos somente se houver espaço disponível, ou seja, caso o diretório de backup esteja cheio os novos registros enviados para o diretório de backup não serão salvos.

5.8.3 Atualizações

Na janela "***Atualizações***" é possível configurar o sistema do Aker Report Center para que as atualizações sejam carregadas automaticamente selecionando o período desejado. Ao carregar as atualizações, as mesmas serão exibidas na lista de Atualizações disponíveis, para que o usuário decida qual atualização ele deseja aplicar. Clique na opção "***Aplicar***" para atualizar o sistema.

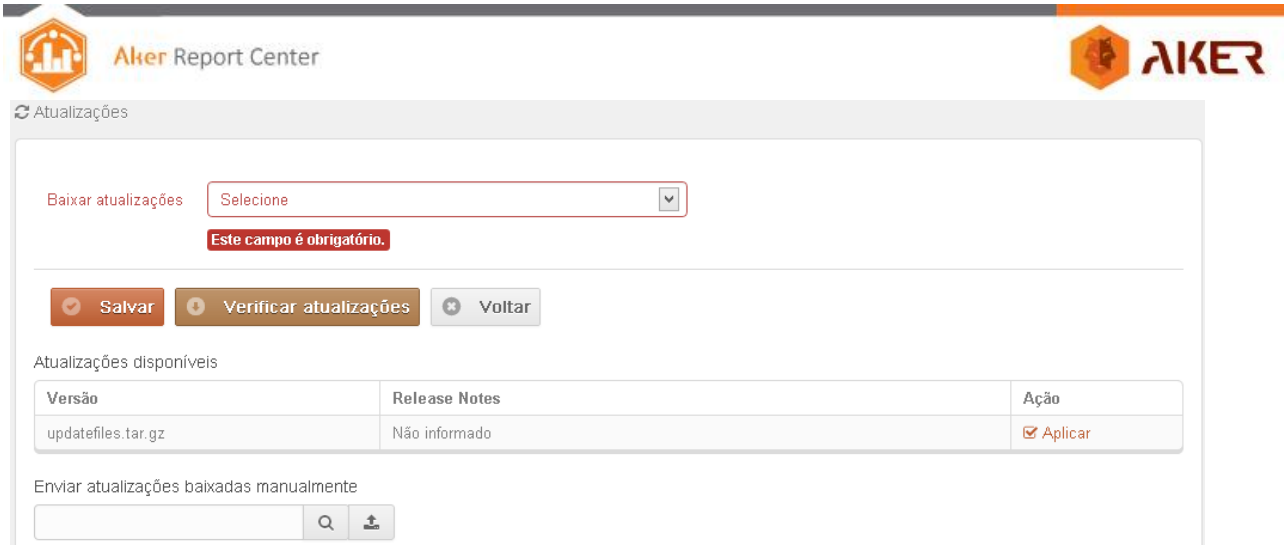


Figura 139 - Atualizações

Baixar atualizações: Neste campo o usuário deve selecionar o período o qual o sistema do Aker Report Center irá baixar as atualizações e disponibiliza-las na lista de atualizações disponível. A seguir as opções de período disponíveis:

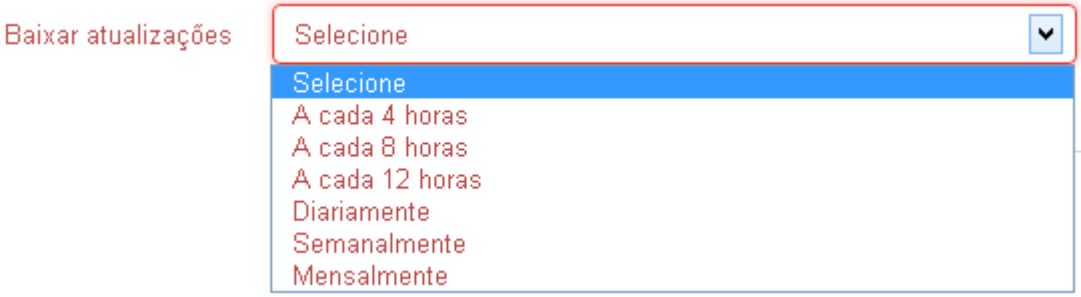


Figura 140 - Opções para baixar atualizações

Enviar atualizações baixadas manualmente: Esta opção permite que o usuário faça o upload de uma atualização manualmente. A atualização será exibida na lista de "***Atualizações disponíveis***" para que a mesma seja aplicada.

5.8.4 E-mail

A janela "***E-mail***" permite que o usuário configure por qual e-mail os relatórios gerados pelo Aker Report Center serão enviados, e também definir uma conta de e-mail que sempre recebera notificações do Aker Report Center como por exemplo, quando a licença do usuário estiver prestes a expirar. A seguir detalhes sobre os campos da janela "***E-mail***".

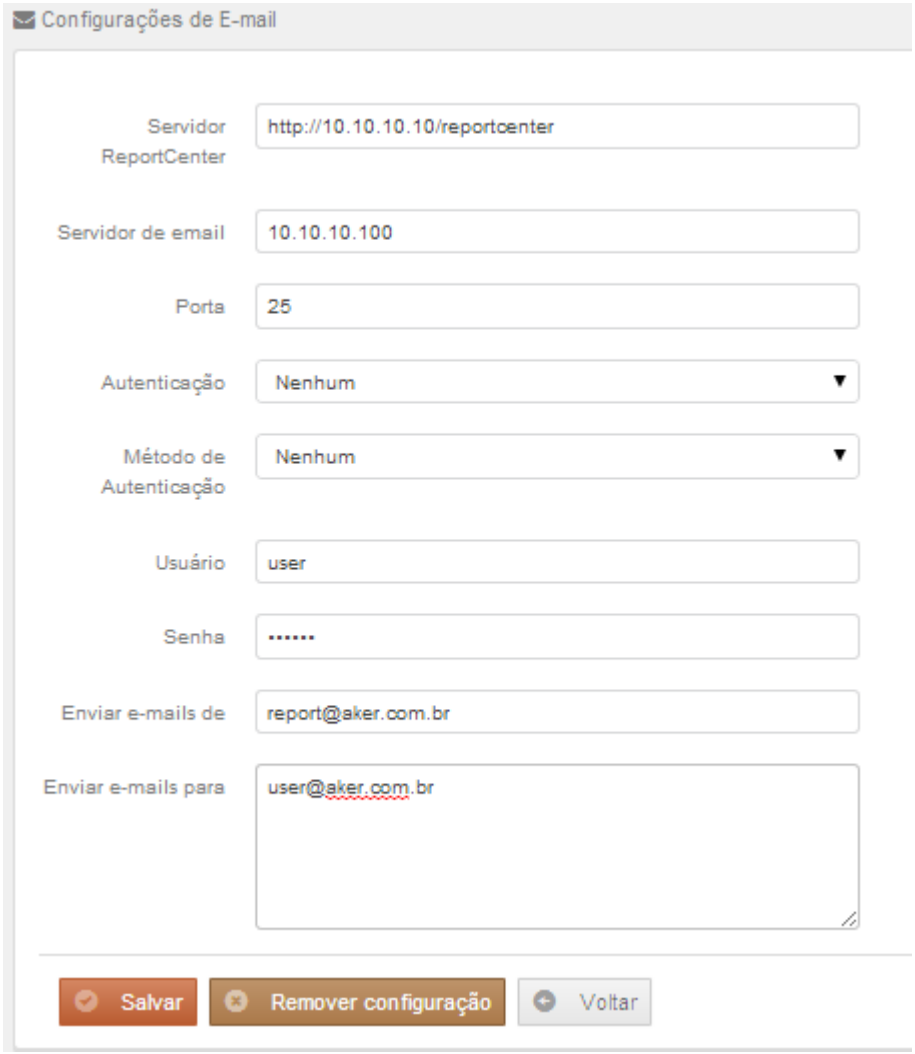


Figura 141 - Configurações de e-mail

Servidor Report Center: Neste campo deve-se inserir o endereço do servidor do Aker Report Center.

Servidor de e-mail: Neste campo deve-se inserir o endereço do servidor de e-mail que será usado para enviar os e-mails do Aker Report Center.

Porta: Neste campo deve-se inserir o número da porta a qual será usada para enviar os e-mails do Aker Report Center

Autenticação: Neste campo define-se a autenticação do usuário será solicitada ou não para baixar o e-mail no servidor.

Método de autenticação: Neste campo deve-se selecionar qual o método de autenticação usado para que o usuário possa fazer o download do e-mail no servidor.

Usuário: Neste campo deve-se inserir o nome do usuário do qual os e-mails do Aker Report Center serão enviados.

Senha: Neste campo deve-se inserir a senha do usuário do qual os e-mails do Aker Report Center serão enviados.

Enviar e-mails de: Neste campo deve-se inserir o e-mail que será usado para enviar s e-mails do Aker Report Center.

Enviar e-mails para: Neste campo deve-se inserir e-mail o qual irá receber o os e-mails do Aker Report Center.

5.8.5 Serviços

Esta janela permite que o usuário configure a quantidade de analisadores (parsers) que estarão funcionando simultaneamente, e as configurações do banco de dados de logs e configuração.

Mais detalhes sobre estes campos a seguir:

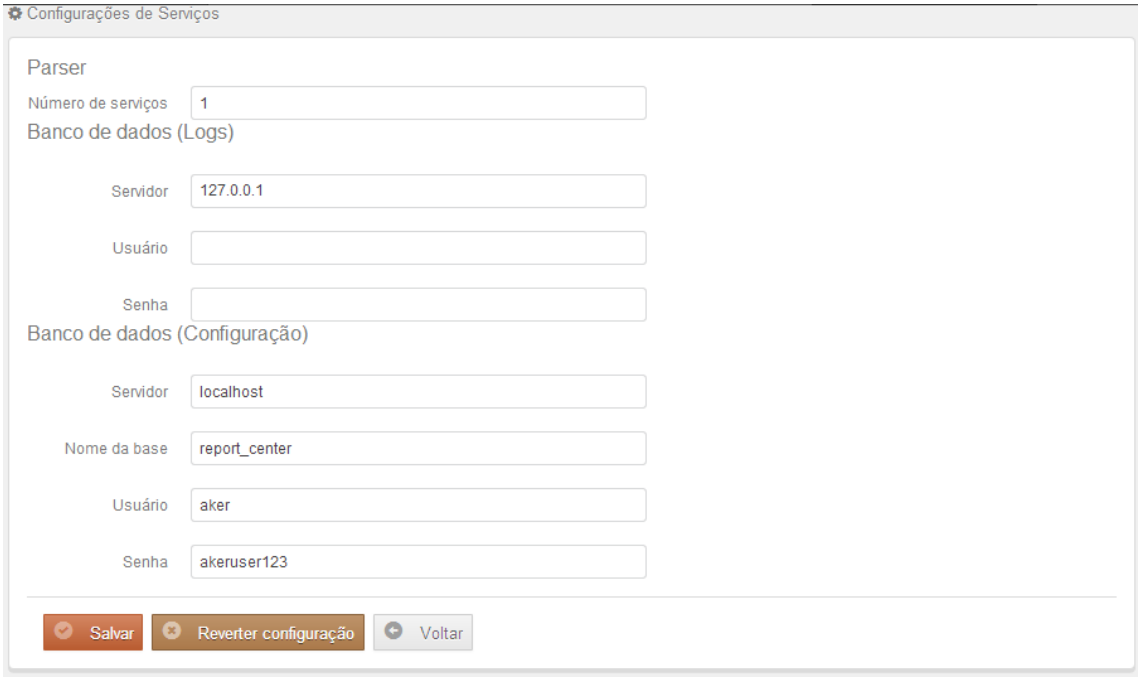


Figura 142 - Janela de configuração de serviços

Parser

- ***Número de serviços:*** Neste campo o usuário deve selecionar a quantidade de analisadores (parsers) estarão rodando simultaneamente (é recomendado que este número seja o mesmo número da quantidade de processadores da máquina)

Banco de dados (logs)

- ***Servidor:*** *Neste campo o usuário deve inserir o endereço do servidor de banco de dados (logs)*

- ***Usuário:*** Neste campo deve-se inserir o nome de usuário para acessar o servidor de banco de dados (este campo pode ser deixado em branco);
- ***Senha:*** Neste campo deve-se a senha de acesso para a autenticação no servidor de banco de dados (este campo pode ser deixado em branco);

Banco de dados (configuração)

- ***Servidor:*** *Neste campo o usuário deve inserir o endereço do servidor de banco de dados (configuração)*
- ***Nome da base:*** Neste campo deve ser inserido o nome do banco de dados de configuração o padrão é report center;
- ***Usuário:*** Neste campo deve-se inserir o nome de usuário para acessar o servidor de banco de dados;
- ***Senha:*** Neste campo deve-se a senha de acesso para a autenticação no servidor de banco de dados;

5.9 *Ajuda*

O menu "Ajuda" permite que o usuário tenha acesso ao manual do Aker Report Center em dois cliques, e também tire suas dúvidas e entre em debates no Fórum da Aker.

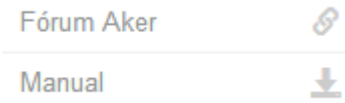


Figura 143 - Menu Ajuda

5.10 *Opções de gerenciamento da conta do usuário*

Estas opções ficam localizadas no lado superior direito da tela, e por meio delas o usuário pode visualizar ou alterar suas informações de forma rápida ou sair do sistema.

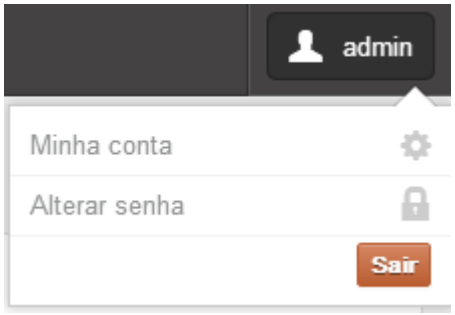


Figura 144 - Opções do usuário

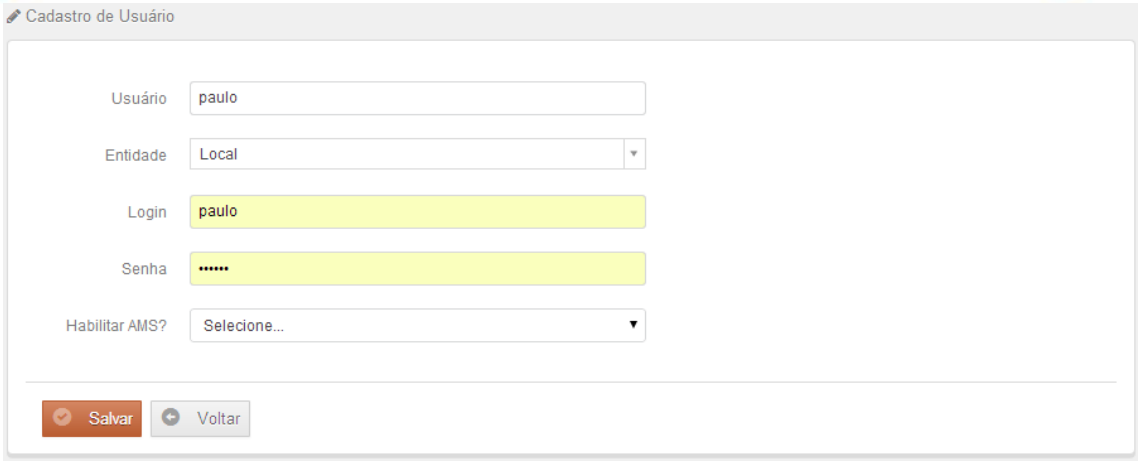


Figura 145 - Minha conta

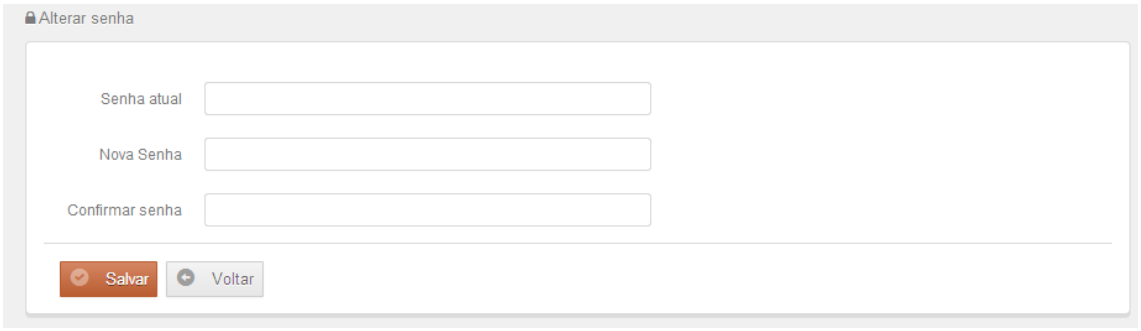


Figura 146 - Alterar Senha